TM Forum Specification

# Digital Identity Management API User Guide

**TMF720**

| | |
|---|---|
| **Maturity Level: General available (GA)** | **Team Approved Date: 14-Nov-2024** |
| **Release Status: Preview** | **Approval Status: Team Approved** |
| **Version 5.0.0** | **IPR Mode: RAND** |

# NOTICE



Direct inquiries to the TM Forum office:

181 New Road, Suite 304
Parsippany, NJ 07054, USA
Tel No. +1 862 227 1648
TM Forum Web Page: www.tmforum.org

# Table of Contents

# Introduction

The scope of this document is to define the Digital Identity Management API in support of the management of digital identities and security credentials. The Digital Identity Management API provides the ability to manage the specific identity data involved in the authentication of a security principal (e.g., user, group, process, application program) to which access rights are granted. The Digital Identity Management API complies with the Open API standards and patterns. The API is described using standard TM Forum approach to API definition. The API data model is derived from the following Information Framework (SID) aggregated business entity model.

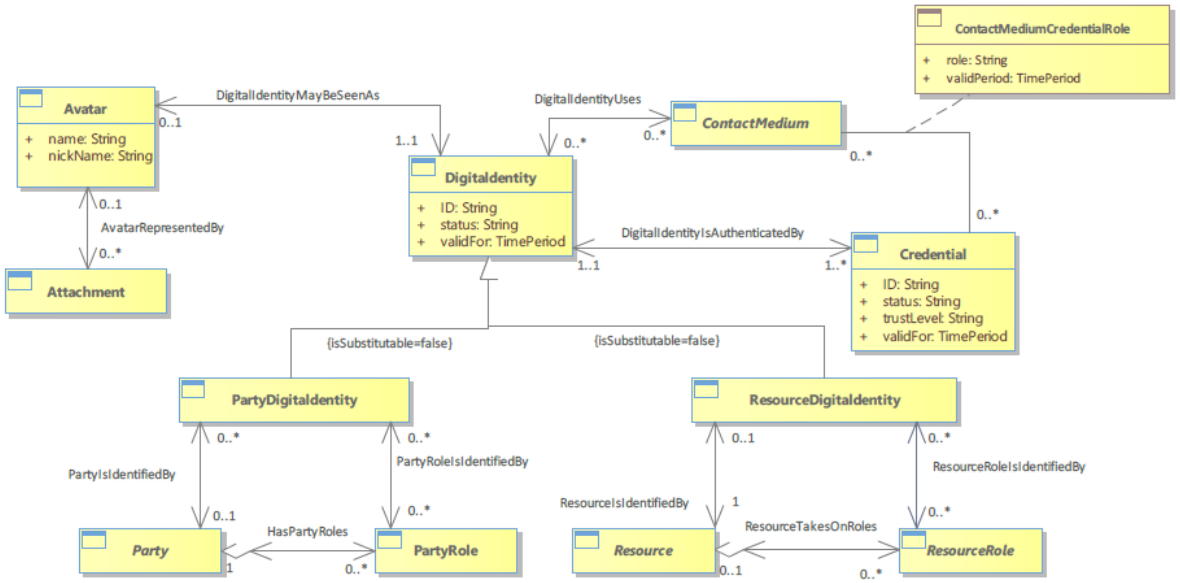


Figure 1. Digital identity overview (SID v23.5 Shared Domain Digital Identity ABE)

The Digital Identity aggregated business entity includes the definition of Digital Identity and Credential entities.

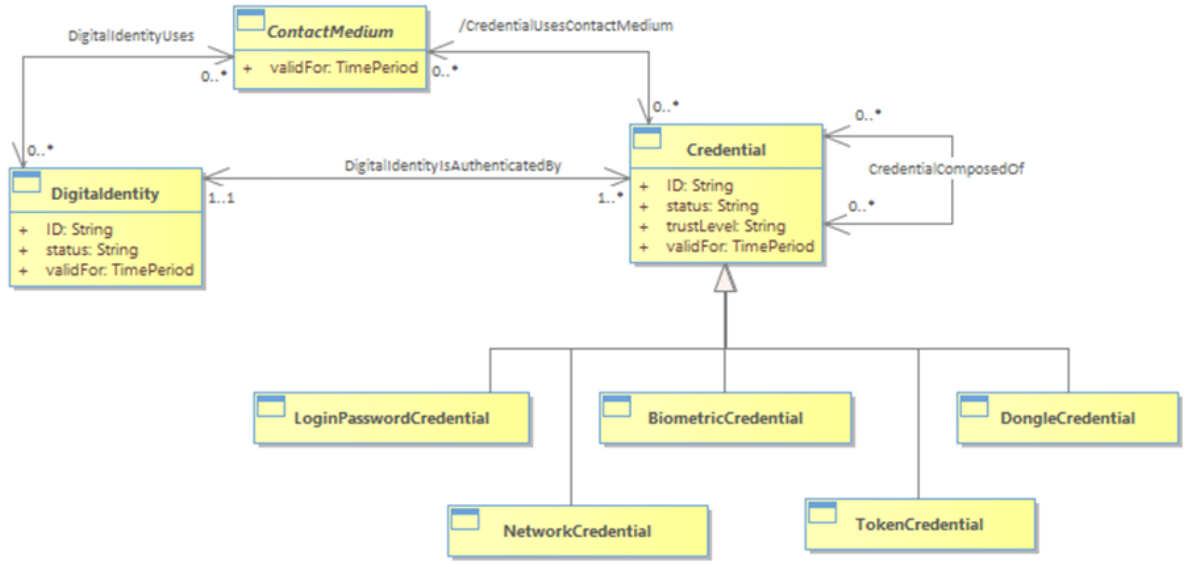

Figure 2. Credential hierarchy (SID v23.5 Shared Domain Digital Identity ABE)

**Digital Identity** refers to the information and characteristics that uniquely identify a security principal (e.g., individual, group, device, software component) in the digital realm. It is the online representation of a party or resource and includes various attributes and credentials associated with them.

Digital identities play a crucial role in ensuring trust, security, and privacy in digital transactions and interactions. They allow security principals (e.g., user, group, process, application program) to prove their identity and establish a level of confidence with other parties involved in digital exchanges.

Various authentication methods, such as passwords, biometrics (fingerprint, facial recognition), hardware tokens, or cryptographic keys, are employed to validate digital identities and protect against unauthorized access or identity theft.

A digital identity enables identification/authentication of party or resource to allow party or resource to use their permissions.

**Party Digital Identity** A party digital identity enables identification/authentication of a unique individual, or the roles played by the individual. Ideally, the digital identity should be defined at party level, but business use cases may have finer-grainer scope and require a digital identity to identify one- or many-party roles. For example, it can be used to have a digital identity carrying all professional party roles delegated by the employer and another one carrying all party roles played personally as a customer. Party digital identities usually enable human-to-machine system identification/authentication interactions.

**Resource Digital Identity** A resource digital identity enables identification/authentication of a unique resource to address machine-to-machine system interactions. For example, a resource digital identity could be provided to an application to trigger interaction with other system (logistic system triggering automatically order to supplier).

**Digital Identity Attributes** The digital identity needs a unique identifier, a status, and a valid period during which the digital identity can be used.

In the realm of Identity Management, various digital identity status plays a crucial role. Let's explore some of them:

- **Active**: Represents a valid and currently accessible digital identity. Users with an "active" status can log in, access resources, and perform authorized actions.
- **Inactive**: Indicates that a digital identity is temporarily disabled or not in use. Users with an "inactive" status cannot log in or access resources until reactivated.
- **Locked**: A status triggered by multiple failed login attempts. A "locked" identity prevents further login until an administrator intervenes or a specified time elapse.
- **Suspended***: Denotes a temporary suspension due to policy violations or other reasons. Users with a "suspended" status cannot perform actions until the suspension is lifted.
- **Pending Approval**: Refers to newly created identities awaiting approval from administrators. These identities are not yet fully active.
- **Expired** Indicates that an identity's validity period has lapsed. Users with an "expired" status need to renew their credentials or revalidate their identity.

- **Terminated**: Represents a permanently disabled identity. Users with a “terminated” status no longer have access rights.

A digital identity might be seen as an avatar. The avatar is used to welcome when connecting. The avatar might be represented by an attachment such as a picture. The avatar might contain a name and a nickname used to welcome when connecting the user to an app.

At least one credential is needed for an active digital identity to identify/authenticate against the digital identity provider. Multiple contact mediums, such as email or phone might be defined at digital identity level to define which contacts can be used for identity account recovery, password reset or "two-factor" authentication.

For example, multiple contact mediums might also be defined at credential level to keep track of contacts used in a password reset or identity login recovery process.

**Security Credential**

The credential is composed by a unique identifier, a status, and a valid period during which the credential can be used. In addition, the credential carries a trust level specifying the credential reliability level. According to the level some permissions might be available or not. For example, with a low level of trust, a customer won’t have the right to buy something.

Here’s a list of common security credential statuses that are often used in an Identity Management platform:

- **Active**: The credential is currently active and can be used for authentication.
- **Inactive**: The credential is inactive and cannot be used for authentication. This status might occur if the user requested to deactivate the credential temporarily.
- **Expired**: The credential has passed its expiration date and cannot be used for authentication. Users may need to renew or update their credential to regain access.
- **Locked**: The credential has been temporarily locked due to multiple failed authentication attempts or security policy violations. This status prevents the credential from being used until it’s unlocked by an administrator or through a predefined process.
- **Revoked**: The credential has been permanently revoked, usually due to security concerns or policy violations. Once revoked, the credential cannot be used for authentication and may require additional actions to reinstate.
- **Pending**: The credential is awaiting approval or activation. This status is common for newly created credentials that require administrative review or user verification before becoming active.
- **Suspended**: The credential has been temporarily suspended, often due to a security investigation or compliance issue. While suspended, the credential cannot be used for authentication until the suspension is lifted.
- **Disabled**: Similar to inactive, this status indicates that the credential is currently disabled and cannot be used for authentication. However, unlike inactive, disabled status may imply a more permanent state or administrative action.
- **Unverified**: The credential has been created but not yet verified. Users may need to complete additional steps to verify their identity before the credential becomes active.

- **Compromised**: The credential has been compromised or suspected of being compromised. This status is used to indicate potential security breaches, and immediate action is required to mitigate risks, such as resetting the credential or investigating further.

In this API, some credential specializations are provided, but additional specializations could be provided by a specific implementation of the API. Listed here are the types of Credentials currently supported:

- **Login Password Credential**: A login password credential defines needed data to authenticate an identity with a login and a password.
- **Network Credential**: A network credential is an implicit credential (automatically retrieved via network access like MSISDN, IP address). It may provide a lower level of confidence than a login password credential for example. Thus, some permissions requesting a high level of confidence might not be available.
- **Biometric Credential**: A biometric credential uses biometric information such as fingerprint, iris, face, or voice.
- **Token Credential**: Token credential corresponds to a link with a digital identity provided by an external digital identity provider such as OpenID, Google ID. The link can be done only if the digital identity provider is a partner from the CSP. A token credential allows to navigate from the partner website to the CSP website without having to identify/authenticate again. Token credential can also be used as system generated security codes issued for password resets, login recovery and "two-factor" authentication purposes.
- **Dongle Credential**: Dongle credential uses a hardware (dongle) that connects to a port on another device to identify / authenticate. In some cases, an additional password might be required and checked on the dongle.

The Digital Identity Management API provides the following capabilities for the management of the digital identities and security credentials used in the identification/authentication of a security principal.

- Management of Digital Identities
- The Digital Identity Management API provides the capability to manage the digital identity data such as:
- Digital identity lifecycle, contact mediums and avatar.
- Security credentials such as login password, network, biometric, token and dongle credentials.

**Digital Identity Global Party and Resource Domain Overview** Digital Identity API (TMF720) plays an important role in the global party and resource domains relating to Role Permission API (TMF672), Party API (TMF632), Party Role API (TMF669), Federated Identity API (TMF691), Resource Inventory API (TMF639) and Resource Role API (TMF768), to managing and controlling access to information and resources within an organization or network.

In summary, these TM Forum Open APIs are related to managing parties, resources and their associated roles and digital identities within a network, as well as controlling access to information and resources through user roles and permissions. They provide a standardized

way for organizations to manage these processes and enable integration with other systems. Following diagram illustrates the digital identity in a global party and resource domains overview, referencing related TM Forum Open APIs and data model entities.

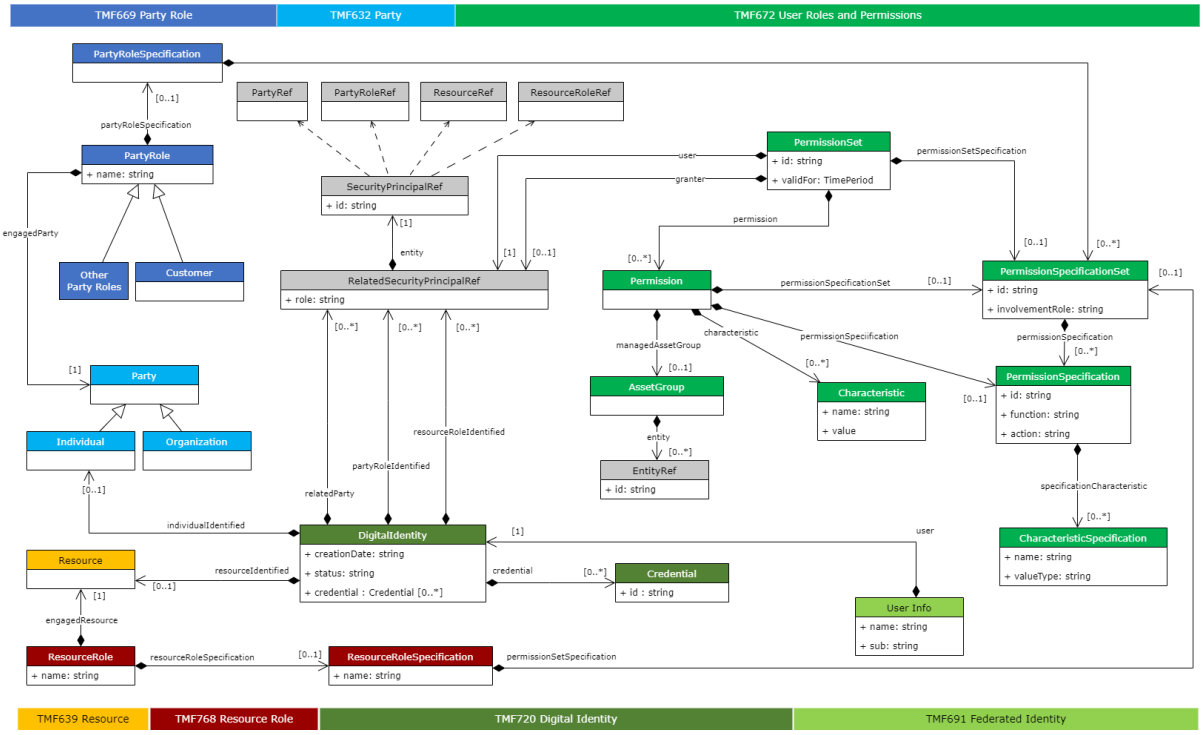


Figure 3. Digital identity global party and resource domain overview

# Sample Use Cases

The Digital Identity Management API provides to manage the digital identities and security credentials.

Some examples use cases are:

- **UC1**: As a potential new customer, Mr. Thomas Anderson needs to create his "account" and provides all the requested information, so that he can be identified/authenticated and recognized for his further interactions with the CSP. Detailed information about this use case can be found here TMFS001 Use Case: New Party – Create your own account v4.0.3 – TM Forum. Sensitive credentials data, such as passwords MUST be omitted from responses. As an example, at the end of the use case the information created will be:

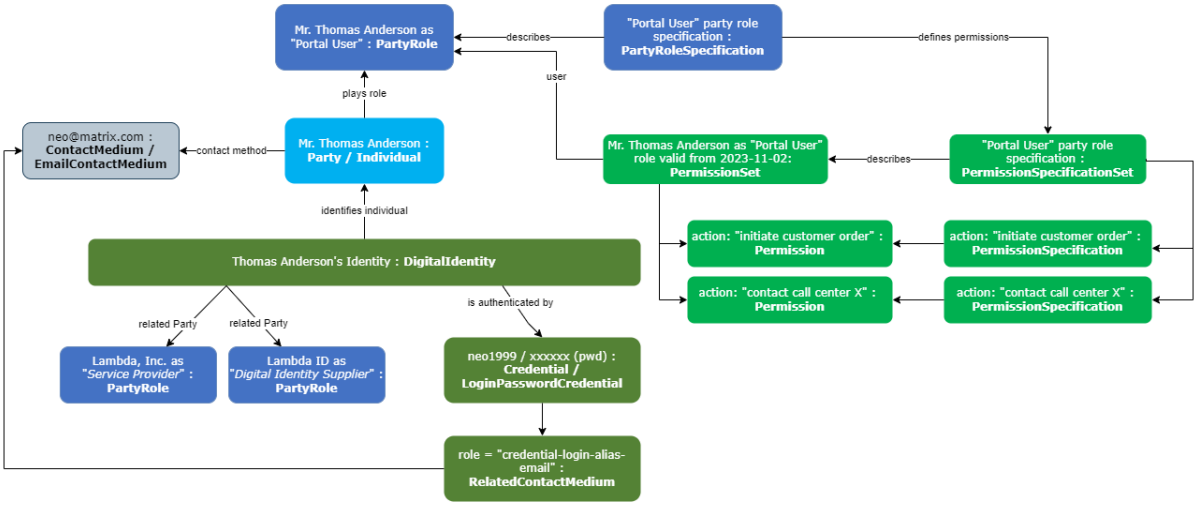


Figure 4. TMFS001 New Party Information Created example

- **UC2**: An Administration User of an Identity and Access Management (IAM) system creating a new digital identity on behalf of the CSP customer, within a digital birth process.
- **UC3**: An Administration User of an Identity and Access Management (IAM) system creating a new digital identity for a Product Catalog Management Web Application that needs to access protected resources such as TMF620 Product Catalog API. As an example, at the end of the use case the information created will be:

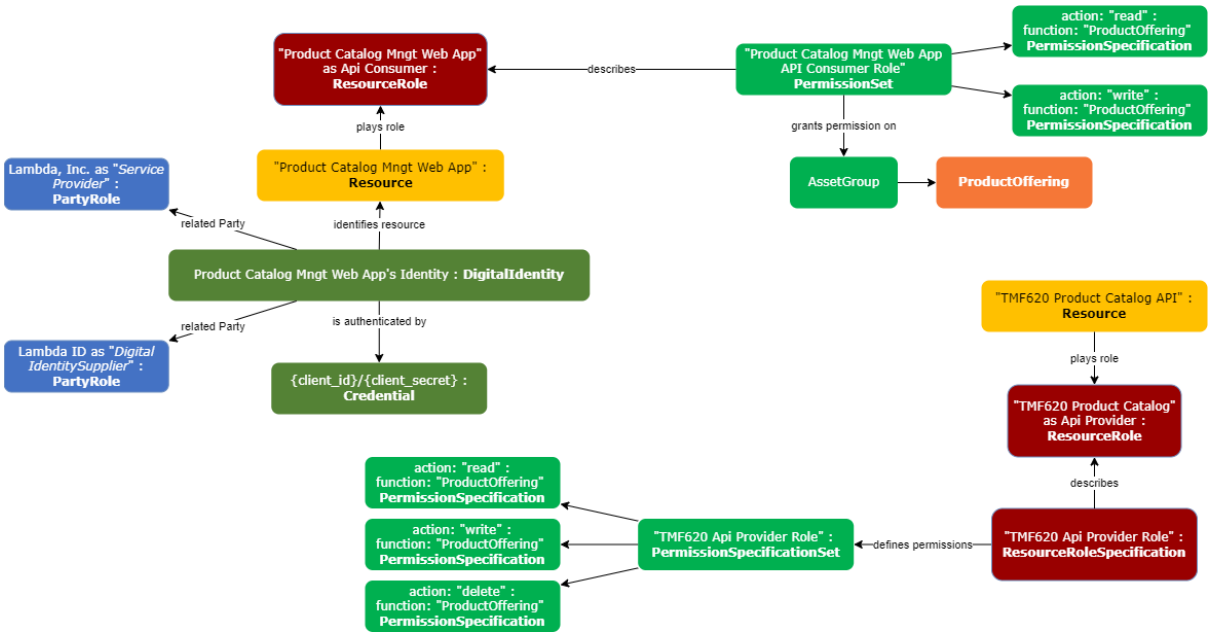


Figure 5. Product Catalog Management Web App Api Consumer example

- **UC4**: An Administration User of an Identity and Access Management (IAM) system is searching for digital identities to manage and monitor digital identities information, such as contact mediums used to recover digital identity account (username recovery or password reset) or to be used for "two-factor" authentication purpose. Sensitive credentials data, such as passwords MUST be omitted from responses. As an example of password reset, at the end of the use case the information created will be:

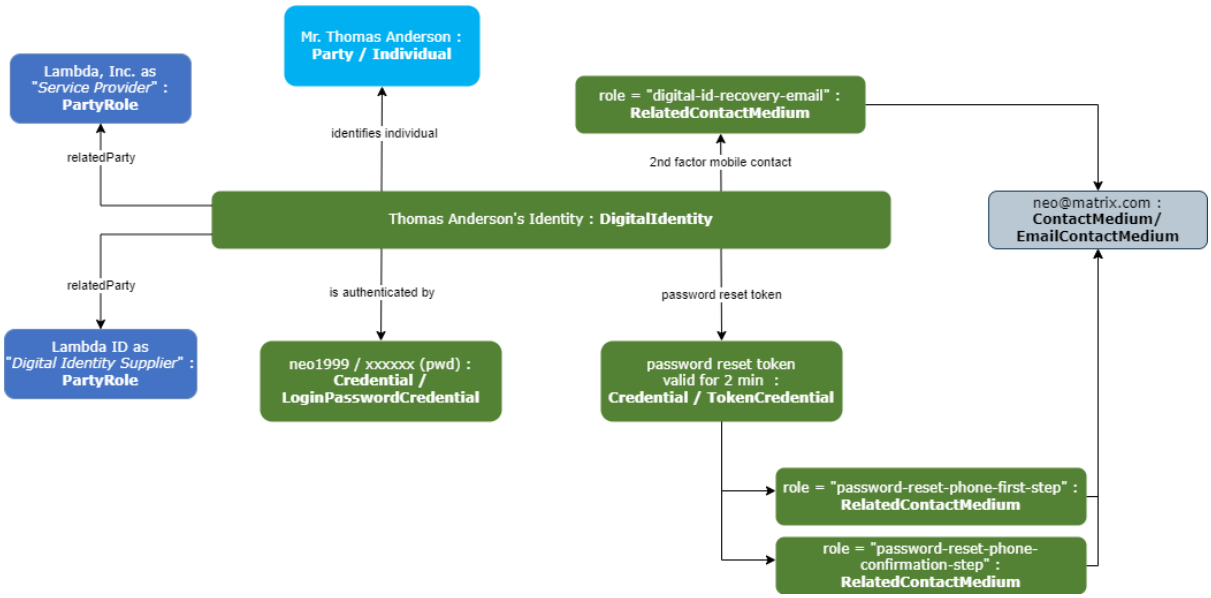


Figure 6. Password Reset Information Created example

As an example of "two-factor" authentication, at the end of the use case the information created will be:

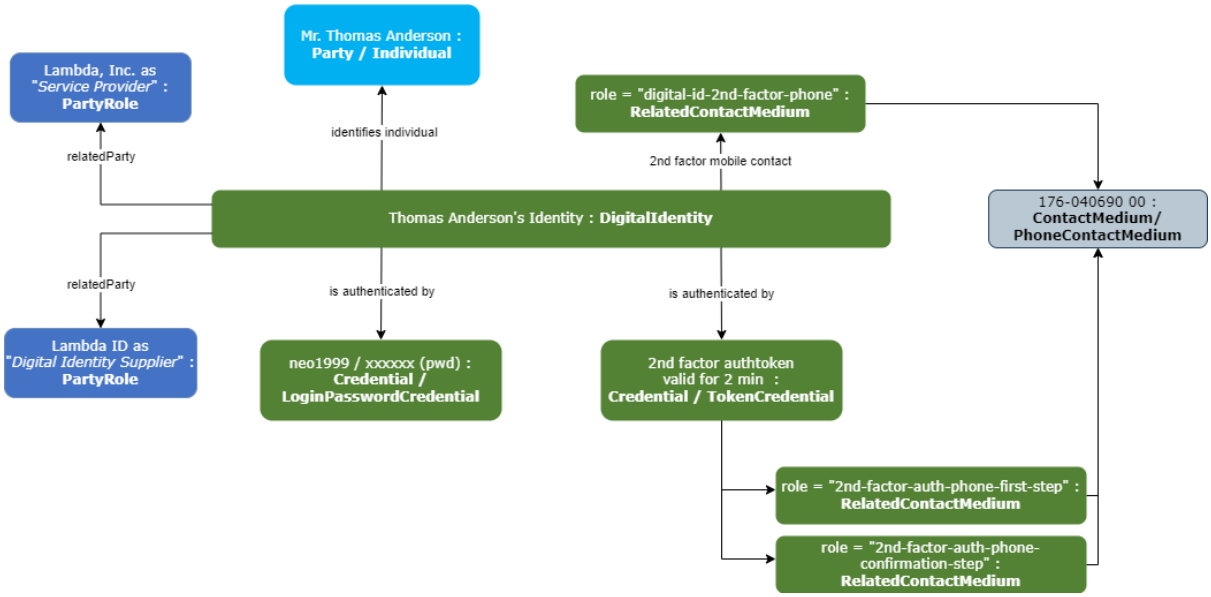


Figure 7. "Two-factor" Authentication Information Created example

# Support of polymorphism and extension patterns

Support of polymorphic collections and types and schema based extension is provided by means of a list of generic meta-attributes that we describe below. Polymorphism in collections occurs when entities inherit from base entities, for instance a BillingAccount and SettlementAccount inheriting properties from the abstract Account entity.

Generic support of polymorphism and pattern extensions is described in the TMF API Guidelines, Part 2 (TMF630).

The @type attribute provides a way to represent the actual class type of an entity. For example, within a list of Account instances some may be instances of BillingAccount where other could be instances of SettlementAccount. The @type gives this information. All resources and sub-resources of this API have a @type attributes that can be provided when this is useful.

The @referredType can be used within reference entities (like for instance an AccountRef object) to explicitly denote the actual entity type of the referred class. Notice that in reference entities the @type, when used, denotes the class type of the reference itself, such as BillingAccountRef or SettlementAccountRef, and not the class type of the referred object. However since reference classes are rarely sub-classed, @type is generally not useful in reference objects.

The @schemaLocation property can be used in resources to allow specifying user-defined properties of an Entity or to specify the expected characteristics of an entity.

The @baseType attribute gives a way to provide explicitly the base of class of a given resource that has been extended.

# RESOURCE MODEL

## Managed Entity and Task Resource Models

### DigitalIdentity resource

DigitalIdentity is a class that allow to describe a digital identity for an individual or a resource or a specific party role or a specific resource role. One of these four MUST be provided. If an individual or resource is provided, this identity will be for all her/his/its party roles or resource roles. To avoid confusion it is recommended to not provide partyRoleIdentified in case party is provided, and to not provide resourceRoleIdentified in case resource is provided.

**Resource model**

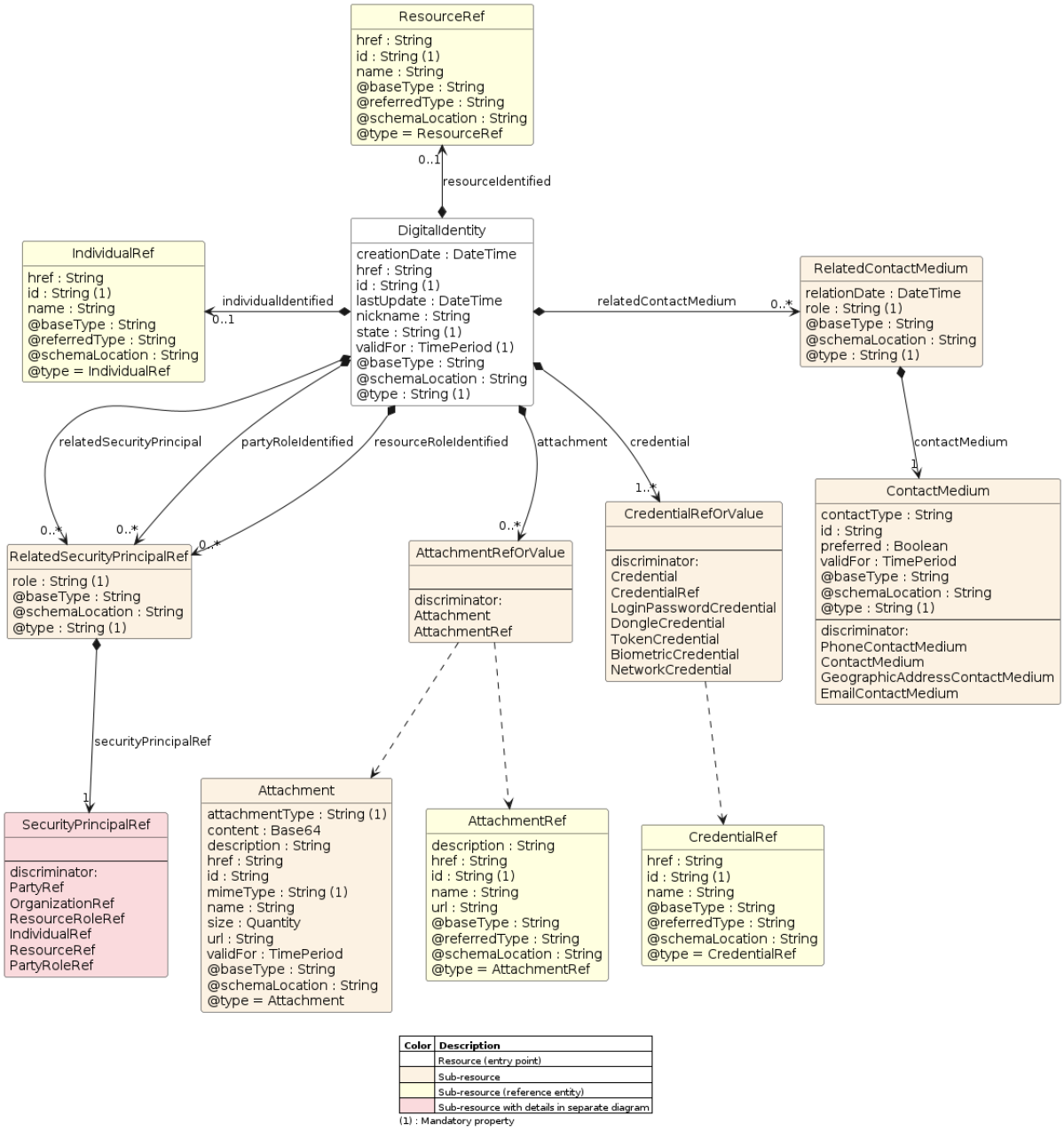


*Figure 1 - DigitalIdentity*

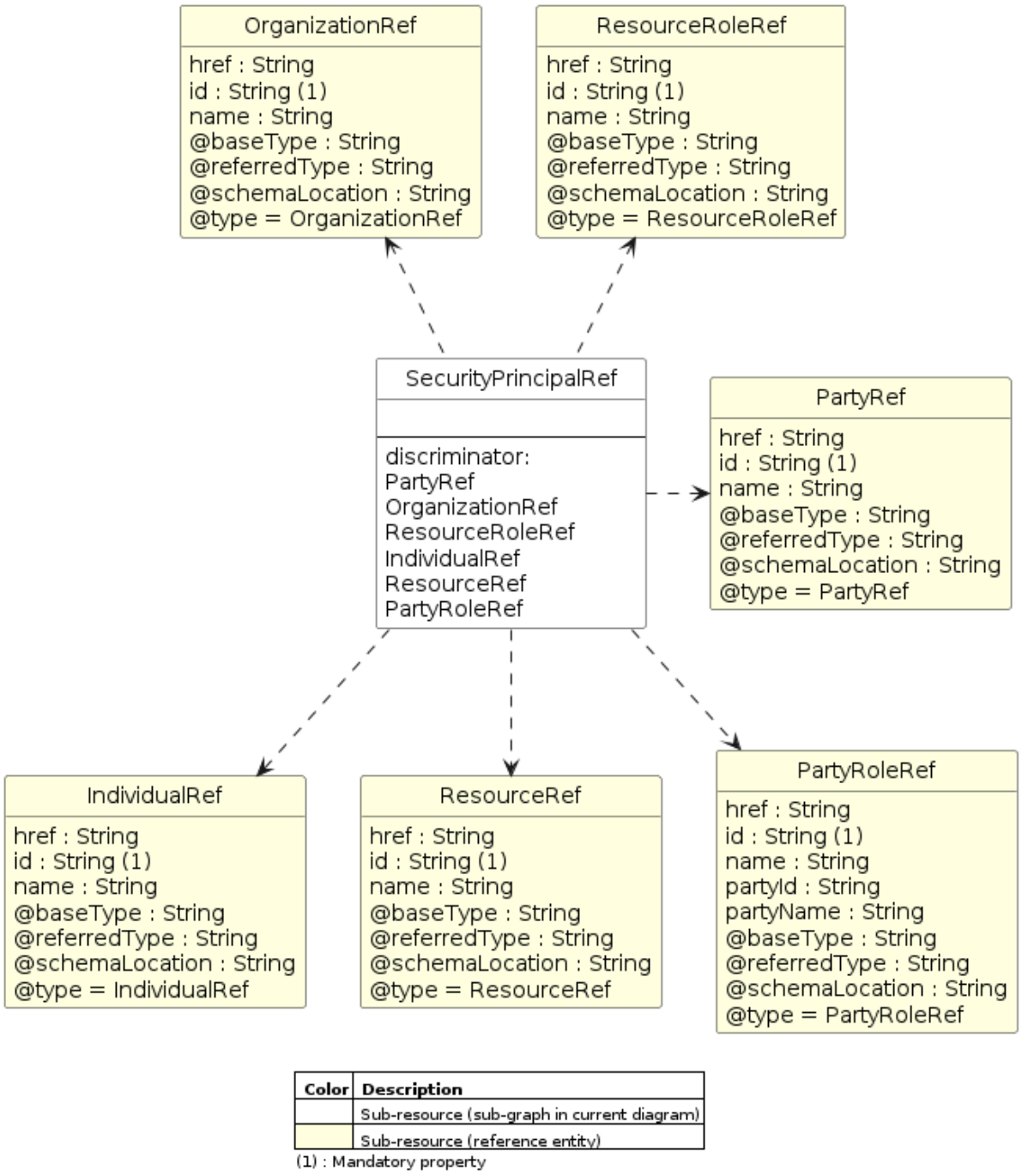


*Figure 2 - SecurityPrincipalRef*

## Field descriptions

### DigitalIdentity fields

| | |
|---|---|
| attachment | An AttachmentRefOrValue. The polymorphic attributes @type, @schemaLocation & @referredType are related to the Attachment entity and not the AttachmentRefOrValue class itself. |
| creationDate | A DateTime. Date and time of the Digital Identity creation (timestamp). |

| | |
|---|---|
| credential | A CredentialRefOrValue. The polymorphic attributes @type, @schemaLocation & @referredType are related to the Credential entity and not the CredentialRefOrValue class itself. |
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| individualIdentified | An IndividualRef. |
| lastUpdate | A DateTime. Date and time of the Digital Identity last update (timestamp). |
| nickname | A String. Nickname associated to this digital identity (like Juanito17 or the QuebecMoose etc…). |
| partyRoleIdentified | A RelatedSecurityPrincipalRef. Related security principal reference. |
| relatedContactMedium | A RelatedContactMedium. A ContactMedium and an associated role such as digital-id-recovery-email, digital-id-recovery-phone, digital-id-2nd-factor-email, digital-id-2nd-factor-phone, credential-login-alias-email, credential-login-alias-phone. |
| relatedSecurityPrincipal | A RelatedSecurityPrincipalRef. Related security principal reference. |
| resourceIdentified | A ResourceRef. Resource reference, for when Resource is used by other entities. |
| resourceRoleIdentified | A RelatedSecurityPrincipalRef. Related security principal reference. |
| state | A String. Digital Identity states: Active (Represents a valid and currently accessible digital identity. Users with an active status can log in, access resources, and perform authorized actions.), Inactive (Indicates that a digital identity is temporarily disabled or not in use. Users with an inactive status cannot log in or access resources until reactivated.), Locked (A status triggered by multiple failed login attempts. A locked identity prevents further login until an administrator intervenes or a specified time elapses.), Suspended (Denotes a temporary suspension due to policy violations or other reasons. Users with a suspended status cannot perform actions until the suspension is lifted.), Pending Approval (Refers to newly created identities awaiting approval from administrators. These identities are not yet fully active.), Expired (Indicates that an identity's validity period has lapsed. Users with an expired status need to renew their credentials or revalidate their identity.), Terminated (Represents a permanently disabled identity. Users with a ?terminated? status no longer have access rights.). |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### RelatedContactMedium sub-resource fields

| | |
|---|---|
| contactMedium | A ContactMedium. Indicates the contact medium that could be used to contact the party. This is an abstract base class, the actual value is in one of the strongly-typed subclasses : EmailContactMedium, FaxContactMedium, PhoneContactMedium, GeographicAddressContactMedium, SocialMediaContactMedium…<br><br>ContactMedium can be instanciated as<br>* EmailContactMedium<br>* GeographicAddressContactMedium<br>* PhoneContactMedium |
| relationDate | A DateTime. Date and time when related contact medium was created. |
| role | A String. Role played by related contact medium. E.g: digital-id-recovery-email, digital-id-recovery-phone, digital-id-2nd-factor-email, digital-id-2nd-factor-phone, credential-login-alias-email, credential-login-alias-phone. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### RelatedSecurityPrincipalRef sub-resource fields

| | |
|---|---|
| role | A String. |
| securityPrincipalRef | A SecurityPrincipalRef. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### IndividualRef sub-resource fields

| | |
|---|---|
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| name | A String. Name of the referred entity. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @referredType | A String. The actual type of the target instance when needed for disambiguation. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |

| | |
|---|---|
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### ResourceRef sub-resource fields

| | |
|---|---|
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| name | A String. Name of the referred entity. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @referredType | A String. The actual type of the target instance when needed for disambiguation. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### Attachment sub-resource fields

| | |
|---|---|
| attachmentType | A String. A business characterization of the purpose of the attachment, for example logo, instructionManual, contractCopy. |
| content | A Base64. The actual contents of the attachment object, if embedded, encoded as base64. |
| description | A String. A narrative text describing the content of the attachment. |
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| mimeType | A String. A technical characterization of the attachment content format using IETF Mime Types. |
| name | A String. The name of the attachment. |
| size | A Quantity. An amount in a given unit. |
| url | A String. Uniform Resource Locator, is a web page address (a subset of URI). |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### AttachmentRef sub-resource fields

| | |
|---|---|
| description | A String. A narrative text describing the content of the attachment. |
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| name | A String. Name of the referred entity. |
| url | A String. Link to the attachment media/content. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @referredType | A String. The actual type of the target instance when needed for disambiguation. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### Credential sub-resource fields

| | |
|---|---|
| creationDate | A DateTime. Date and time of the Credential creation (timestamp). |
| digitalIdentity | A DigitalIdentityRef. DigitalIdentity reference. |
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| lastUpdate | A DateTime. Date and time of the Credential last update (timestamp). |
| relatedContactMedium | A RelatedContactMedium. A ContactMedium and an associated role such as digital-id-recovery-email, digital-id-recovery-phone, digital-id-2nd-factor-email, digital-id-2nd-factor-phone, credential-login-alias-email, credential-login-alias-phone. |

| | |
|---|---|
| state | A String. Active (The credential is currently active and can be used for authentication.), Inactive (The credential is inactive and cannot be used for authentication. This status might occur if the user requested to deactivate the credential temporarily), Expired (The credential has passed its expiration date and cannot be used for authentication. Users may need to renew or update their credential to regain access.), Locked (The credential has been temporarily locked due to multiple failed authentication attempts or security policy violations. This status prevents the credential from being used until it's unlocked by an administrator or through a predefined process.), Revoked (The credential has been permanently revoked, usually due to security concerns or policy violations. Once revoked, the credential cannot be used for authentication and may require additional actions to reinstate.) Pending (The credential is awaiting approval or activation. This status is common for newly created credentials that require administrative review or user verification before becoming active.), Suspended )The credential has been temporarily suspended, often due to a security investigation or compliance issue. While suspended, the credential cannot be used for authentication until the suspension is lifted.), Disabled (Similar to inactive, this status indicates that the credential is currently disabled and cannot be used for authentication. However, unlike inactive, disabled status may imply a more permanent state or administrative action.), Unverified (The credential has been created but not yet verified. Users may need to complete additional steps to verify their identity before the credential becomes active.), Compromised (The credential has been compromised or suspected of being compromised. This status is used to indicate potential security breaches, and immediate action is required to mitigate risks, such as resetting the credential or investigating further.). |
| trustLevel | A String. A level of assurance associated with this credential - this could be used to limit/allow specific permission based on this trust level. |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |
| | Credential can be instanciated as<br>* BiometricCredential<br>* DongleCredential<br>* LoginPasswordCredential<br>* NetworkCredential<br>* TokenCredential |
| attachment | This property is present in subclasses |
| biometricSubType | This property is present in subclasses |

| | |
|---|---|
| biometricType | This property is present in subclasses |
| login | This property is present in subclasses |
| password | This property is present in subclasses |
| resource | This property is present in subclasses |
| securityKeyId | This property is present in subclasses |
| securityKeyProvider | This property is present in subclasses |
| securityKeyType | This property is present in subclasses |
| tokenCredential | This property is present in subclasses |

### CredentialRef sub-resource fields

| | |
|---|---|
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| name | A String. Name of the referred entity. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @referredType | A String. The actual type of the target instance when needed for disambiguation. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### LoginPasswordCredential sub-resource fields

| | |
|---|---|
| creationDate | A DateTime. Date and time of the Credential creation (timestamp). |
| digitalIdentity | A DigitalIdentityRef. DigitalIdentity reference. |
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| lastUpdate | A DateTime. Date and time of the Credential last update (timestamp). |
| login | A String. Credential login. |
| password | A String. Credential password - must be in write only. |
| relatedContactMedium | A RelatedContactMedium. A ContactMedium and an associated role such as digital-id-recovery-email, digital-id-recovery-phone, digital-id-2nd-factor-email, digital-id-2nd-factor-phone, credential-login-alias-email, credential-login-alias-phone. |

| | |
|---|---|
| state | A String. Active (The credential is currently active and can be used for authentication.), Inactive (The credential is inactive and cannot be used for authentication. This status might occur if the user requested to deactivate the credential temporarily), Expired (The credential has passed its expiration date and cannot be used for authentication. Users may need to renew or update their credential to regain access.), Locked (The credential has been temporarily locked due to multiple failed authentication attempts or security policy violations. This status prevents the credential from being used until it's unlocked by an administrator or through a predefined process.), Revoked (The credential has been permanently revoked, usually due to security concerns or policy violations. Once revoked, the credential cannot be used for authentication and may require additional actions to reinstate.) Pending (The credential is awaiting approval or activation. This status is common for newly created credentials that require administrative review or user verification before becoming active.), Suspended )The credential has been temporarily suspended, often due to a security investigation or compliance issue. While suspended, the credential cannot be used for authentication until the suspension is lifted.), Disabled (Similar to inactive, this status indicates that the credential is currently disabled and cannot be used for authentication. However, unlike inactive, disabled status may imply a more permanent state or administrative action.), Unverified (The credential has been created but not yet verified. Users may need to complete additional steps to verify their identity before the credential becomes active.), Compromised (The credential has been compromised or suspected of being compromised. This status is used to indicate potential security breaches, and immediate action is required to mitigate risks, such as resetting the credential or investigating further.). |
| trustLevel | A String. A level of assurance associated with this credential - this could be used to limit/allow specific permission based on this trust level. |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### DongleCredential sub-resource fields

| | |
|---|---|
| creationDate | A DateTime. Date and time of the Credential creation (timestamp). |
| digitalIdentity | A DigitalIdentityRef. DigitalIdentity reference. |
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |

| | |
|---|---|
| lastUpdate | A DateTime. Date and time of the Credential last update (timestamp). |
| relatedContactMedium | A RelatedContactMedium. A ContactMedium and an associated role such as digital-id-recovery-email, digital-id-recovery-phone, digital-id-2nd-factor-email, digital-id-2nd-factor-phone, credential-login-alias-email, credential-login-alias-phone. |
| securityKeyId | A String. A security key identifier, also known as the credential ID, is a unique identifier associated with a specific security key. It is generated during the enrollment process when a security key is registered with a service or platform. The security key identifier is used to identify and authenticate the security key during subsequent login attempts. It serves as a reference to the corresponding cryptographic key pair stored securely within the security key. |
| securityKeyProvider | A String. A security key provider refers to an entity, such as a manufacturer, vendor, or service provider, that supplies or offers security keys to end-users or organizations. These providers may develop and produce the physical security key devices or provide the associated software, services, and infrastructure necessary for their usage. Security key providers play a crucial role in ensuring the availability, quality, and security of the security keys and associated components, including firmware updates, key management systems, and authentication protocols. They may also offer additional services like customer support, integration assistance, and compliance with industry standards. |
| securityKeyType | A String. The security key type refers to the classification or category of a security key based on its underlying technology or functionality. Examples: USB security key, NFC security key. |

| | |
|---|---|
| state | A String. Active (The credential is currently active and can be used for authentication.), Inactive (The credential is inactive and cannot be used for authentication. This status might occur if the user requested to deactivate the credential temporarily), Expired (The credential has passed its expiration date and cannot be used for authentication. Users may need to renew or update their credential to regain access.), Locked (The credential has been temporarily locked due to multiple failed authentication attempts or security policy violations. This status prevents the credential from being used until it's unlocked by an administrator or through a predefined process.), Revoked (The credential has been permanently revoked, usually due to security concerns or policy violations. Once revoked, the credential cannot be used for authentication and may require additional actions to reinstate.) Pending (The credential is awaiting approval or activation. This status is common for newly created credentials that require administrative review or user verification before becoming active.), Suspended )The credential has been temporarily suspended, often due to a security investigation or compliance issue. While suspended, the credential cannot be used for authentication until the suspension is lifted.), Disabled (Similar to inactive, this status indicates that the credential is currently disabled and cannot be used for authentication. However, unlike inactive, disabled status may imply a more permanent state or administrative action.), Unverified (The credential has been created but not yet verified. Users may need to complete additional steps to verify their identity before the credential becomes active.), Compromised (The credential has been compromised or suspected of being compromised. This status is used to indicate potential security breaches, and immediate action is required to mitigate risks, such as resetting the credential or investigating further.). |
| trustLevel | A String. A level of assurance associated with this credential - this could be used to limit/allow specific permission based on this trust level. |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### TokenCredential sub-resource fields

| | |
|---|---|
| creationDate | A DateTime. Date and time of the Credential creation (timestamp). |
| digitalIdentity | A DigitalIdentityRef. DigitalIdentity reference. |
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |

| | |
|---|---|
| lastUpdate | A DateTime. Date and time of the Credential last update (timestamp). |
| login | A String. Credential login. |
| relatedContactMedium | A RelatedContactMedium. A ContactMedium and an associated role such as digital-id-recovery-email, digital-id-recovery-phone, digital-id-2nd-factor-email, digital-id-2nd-factor-phone, credential-login-alias-email, credential-login-alias-phone. |
| state | A String. Active (The credential is currently active and can be used for authentication.), Inactive (The credential is inactive and cannot be used for authentication. This status might occur if the user requested to deactivate the credential temporarily), Expired (The credential has passed its expiration date and cannot be used for authentication. Users may need to renew or update their credential to regain access.), Locked (The credential has been temporarily locked due to multiple failed authentication attempts or security policy violations. This status prevents the credential from being used until it's unlocked by an administrator or through a predefined process.), Revoked (The credential has been permanently revoked, usually due to security concerns or policy violations. Once revoked, the credential cannot be used for authentication and may require additional actions to reinstate.) Pending (The credential is awaiting approval or activation. This status is common for newly created credentials that require administrative review or user verification before becoming active.), Suspended )The credential has been temporarily suspended, often due to a security investigation or compliance issue. While suspended, the credential cannot be used for authentication until the suspension is lifted.), Disabled (Similar to inactive, this status indicates that the credential is currently disabled and cannot be used for authentication. However, unlike inactive, disabled status may imply a more permanent state or administrative action.), Unverified (The credential has been created but not yet verified. Users may need to complete additional steps to verify their identity before the credential becomes active.), Compromised (The credential has been compromised or suspected of being compromised. This status is used to indicate potential security breaches, and immediate action is required to mitigate risks, such as resetting the credential or investigating further.). |
| tokenCredential | A String. Token credential identifier. |
| trustLevel | A String. A level of assurance associated with this credential - this could be used to limit/allow specific permission based on this trust level. |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### BiometricCredential sub-resource fields

| | |
|---|---|
| attachment | An AttachmentRefOrValue. The polymorphic attributes @type, @schemaLocation & @referredType are related to the Attachment entity and not the AttachmentRefOrValue class itself. |
| biometricSubType | A String. A biometric sub type when required like for finger: thumb, index, ring , pinkyFinger, etc. |
| biometricType | A String. A biometric type like finger, iris, face, etc… |
| creationDate | A DateTime. Date and time of the Credential creation (timestamp). |
| digitalIdentity | A DigitalIdentityRef. DigitalIdentity reference. |
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| lastUpdate | A DateTime. Date and time of the Credential last update (timestamp). |
| relatedContactMedium | A RelatedContactMedium. A ContactMedium and an associated role such as digital-id-recovery-email, digital-id-recovery-phone, digital-id-2nd-factor-email, digital-id-2nd-factor-phone, credential-login-alias-email, credential-login-alias-phone. |

| | |
|---|---|
| state | A String. Active (The credential is currently active and can be used for authentication.), Inactive (The credential is inactive and cannot be used for authentication. This status might occur if the user requested to deactivate the credential temporarily), Expired (The credential has passed its expiration date and cannot be used for authentication. Users may need to renew or update their credential to regain access.), Locked (The credential has been temporarily locked due to multiple failed authentication attempts or security policy violations. This status prevents the credential from being used until it's unlocked by an administrator or through a predefined process.), Revoked (The credential has been permanently revoked, usually due to security concerns or policy violations. Once revoked, the credential cannot be used for authentication and may require additional actions to reinstate.) Pending (The credential is awaiting approval or activation. This status is common for newly created credentials that require administrative review or user verification before becoming active.), Suspended )The credential has been temporarily suspended, often due to a security investigation or compliance issue. While suspended, the credential cannot be used for authentication until the suspension is lifted.), Disabled (Similar to inactive, this status indicates that the credential is currently disabled and cannot be used for authentication. However, unlike inactive, disabled status may imply a more permanent state or administrative action.), Unverified (The credential has been created but not yet verified. Users may need to complete additional steps to verify their identity before the credential becomes active.), Compromised (The credential has been compromised or suspected of being compromised. This status is used to indicate potential security breaches, and immediate action is required to mitigate risks, such as resetting the credential or investigating further.). |
| trustLevel | A String. A level of assurance associated with this credential - this could be used to limit/allow specific permission based on this trust level. |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### NetworkCredential sub-resource fields

| | |
|---|---|
| creationDate | A DateTime. Date and time of the Credential creation (timestamp). |
| digitalIdentity | A DigitalIdentityRef. DigitalIdentity reference. |
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |

| | |
|---|---|
| lastUpdate | A DateTime. Date and time of the Credential last update (timestamp). |
| password | A String. Credential password to use resource based credential. Sensitive data such as passwords MUST be ommitted in GET responses. |
| relatedContactMedium | A RelatedContactMedium. A ContactMedium and an associated role such as digital-id-recovery-email, digital-id-recovery-phone, digital-id-2nd-factor-email, digital-id-2nd-factor-phone, credential-login-alias-email, credential-login-alias-phone. |
| resource | A ResourceRef. Resource reference, for when Resource is used by other entities. |
| state | A String. Active (The credential is currently active and can be used for authentication.), Inactive (The credential is inactive and cannot be used for authentication. This status might occur if the user requested to deactivate the credential temporarily), Expired (The credential has passed its expiration date and cannot be used for authentication. Users may need to renew or update their credential to regain access.), Locked (The credential has been temporarily locked due to multiple failed authentication attempts or security policy violations. This status prevents the credential from being used until it's unlocked by an administrator or through a predefined process.), Revoked (The credential has been permanently revoked, usually due to security concerns or policy violations. Once revoked, the credential cannot be used for authentication and may require additional actions to reinstate.) Pending (The credential is awaiting approval or activation. This status is common for newly created credentials that require administrative review or user verification before becoming active.), Suspended )The credential has been temporarily suspended, often due to a security investigation or compliance issue. While suspended, the credential cannot be used for authentication until the suspension is lifted.), Disabled (Similar to inactive, this status indicates that the credential is currently disabled and cannot be used for authentication. However, unlike inactive, disabled status may imply a more permanent state or administrative action.), Unverified (The credential has been created but not yet verified. Users may need to complete additional steps to verify their identity before the credential becomes active.), Compromised (The credential has been compromised or suspected of being compromised. This status is used to indicate potential security breaches, and immediate action is required to mitigate risks, such as resetting the credential or investigating further.). |
| trustLevel | A String. A level of assurance associated with this credential - this could be used to limit/allow specific permission based on this trust level. |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |

| | |
|---|---|
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### ContactMedium sub-resource fields

| | |
|---|---|
| contactType | A String. Type of the contact medium to qualify it like pro email / personal email. This is not used to define the contact medium used. |
| id | A String. Identifier for this contact medium. |
| preferred | A Boolean. If true, indicates that is the preferred contact medium. |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |
| | ContactMedium can be instanciated as<br>* EmailContactMedium<br>* GeographicAddressContactMedium<br>* PhoneContactMedium |
| city | This property is present in subclasses |
| country | This property is present in subclasses |
| emailAddress | This property is present in subclasses |
| geographicAddress | This property is present in subclasses |
| phoneNumber | This property is present in subclasses |
| postCode | This property is present in subclasses |
| stateOrProvince | This property is present in subclasses |
| street1 | This property is present in subclasses |
| street2 | This property is present in subclasses |

### PhoneContactMedium sub-resource fields

| | |
|---|---|
| contactType | A String. Type of the contact medium to qualify it like pro email / personal email. This is not used to define the contact medium used. |
| id | A String. Identifier for this contact medium. |
| phoneNumber | A String. The phone number of the contact. |
| preferred | A Boolean. If true, indicates that is the preferred contact medium. |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |

| | |
|---|---|
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### GeographicAddressContactMedium sub-resource fields

| | |
|---|---|
| city | A String. The city. |
| contactType | A String. Type of the contact medium to qualify it like pro email / personal email. This is not used to define the contact medium used. |
| country | A String. The country. |
| geographicAddress | A GeographicAddressRef. Reference to a Geographic Address. |
| id | A String. Identifier for this contact medium. |
| postCode | A String. Postcode. |
| preferred | A Boolean. If true, indicates that is the preferred contact medium. |
| stateOrProvince | A String. State or province. |
| street1 | A String. Describes the street. |
| street2 | A String. Complementary street description. |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### EmailContactMedium sub-resource fields

| | |
|---|---|
| contactType | A String. Type of the contact medium to qualify it like pro email / personal email. This is not used to define the contact medium used. |
| emailAddress | A String. Full email address in standard format. |
| id | A String. Identifier for this contact medium. |
| preferred | A Boolean. If true, indicates that is the preferred contact medium. |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### GeographicAddressRef sub-resource fields

| | |
|---|---|
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| name | A String. Name of the referred entity. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @referredType | A String. The actual type of the target instance when needed for disambiguation. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### PartyRef sub-resource fields

| | |
|---|---|
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| name | A String. Name of the referred entity. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @referredType | A String. The actual type of the target instance when needed for disambiguation. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### OrganizationRef sub-resource fields

| | |
|---|---|
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| name | A String. Name of the referred entity. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @referredType | A String. The actual type of the target instance when needed for disambiguation. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### ResourceRoleRef sub-resource fields

| | |
|---|---|
| href | A String. Hyperlink reference. |

| | |
|---|---|
| id | A String. Unique identifier. |
| name | A String. Name of the referred entity. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @referredType | A String. The actual type of the target instance when needed for disambiguation. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### PartyRoleRef sub-resource fields

| | |
|---|---|
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| name | A String. Name of the referred entity. |
| partyId | A String. The identifier of the engaged party that is linked to the PartyRole object. |
| partyName | A String. The name of the engaged party that is linked to the PartyRole object. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @referredType | A String. The actual type of the target instance when needed for disambiguation. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### DigitalIdentityRef sub-resource fields

| | |
|---|---|
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| name | A String. Name of the referred entity. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @referredType | A String. The actual type of the target instance when needed for disambiguation. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### Json representation sample(s)

We provide below a JSON representation as example of the 'DigitalIdentity' resource object.

```
{
   "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/digitalIdentity/2391ee4acbc142b1a4b74b4d4ab38152",
   "id": "2391ee4acbc142b1a4b74b4d4ab38152",
   "@type": "DigitalIdentity",
   "nickname": "Neo",
   "state": "Active",
   "validFor": {
      "startDateTime": "2018-09-21T23:20:50.52Z"
   },
   "credential": [
      {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/loginPasswordCredential/41af4b86e0b144cb9099b3d4c3a
b26ae",
         "id": "41af4b86e0b144cb9099b3d4c3ab26ae",
         "@type": "LoginPasswordCredential",
         "@baseType": "Credential",
         "state": "Active",
         "validFor": {
            "startDateTime": "2018-09-21T23:20:50.52Z"
         },
         "trustLevel": "high",
         "relatedContactMedium": [
            {
               "@type": "RelatedContactMedium",
               "role": "credential-login-alias-email",
               "contactMedium": {
                  "@type": "EmailContactMedium",
                  "@baseType": "ContactMedium",
                  "contactType": "private",
                  "id": "b2fe04a7f96e479195a47710abcf72be",
                  "preferred": true,
                  "validFor": {
                     "startDateTime": "2018-09-21T23:20:50.52Z"
                  },
                  "emailAddress": "neo@matrix.com"
               },
               "relationDate": "2018-09-21T23:20:50.52Z"
            },
            {
               "@type": "RelatedContactMedium",
               "role": "credential-login-alias-phone",
               "contactMedium": {
                  "@type": "PhoneContactMedium",
                  "@baseType": "ContactMedium",
                  "contactType": "private",
                  "id": "c0181f3d83e144a59162fd6136a98462",
                  "preferred": true,
                  "validFor": {
                     "startDateTime": "2018-09-21T23:20:50.52Z"
                  },
                  "phoneNumber": "+1 202-918-2132"
               },
               "relationDate": "2018-09-21T23:20:50.52Z"
            }
         ],
         "login": "neo1999",
         "creationDate": "2018-09-21T09:13:16-07:00",
         "lastUpdate": "2018-09-21T23:20:50.52Z"
      }
   ],
```

```
    "relatedContactMedium": [
       {
          "@type": "RelatedContactMedium",
          "role": "digital-id-recovery-email",
          "contactMedium": {
             "@type": "EmailContactMedium",
             "@baseType": "ContactMedium",
             "contactType": "private",
             "id": "b2fe04a7f96e479195a47710abcf72be",
             "preferred": true,
             "validFor": {
                "startDateTime": "2018-09-21T23:20:50.52Z"
             },
             "emailAddress": "neo@matrix.com"
          },
          "relationDate": "2018-09-21T23:20:50.52Z"
       },
       {
          "@type": "RelatedContactMedium",
          "role": "digital-id-recovery-phone",
          "contactMedium": {
             "@type": "PhoneContactMedium",
             "@baseType": "ContactMedium",
             "contactType": "private",
             "id": "60703a48038e4fc9a46bf1459aa3590f",
             "preferred": false,
             "validFor": {
                "startDateTime": "2018-09-21T23:20:50.52Z"
             },
             "phoneNumber": "+1 202-918-2132"
          },
          "relationDate": "2018-09-21T23:20:50.52Z"
       },
       {
          "@type": "RelatedContactMedium",
          "role": "digital-id-2nd-factor-phone",
          "contactMedium": {
             "@type": "PhoneContactMedium",
             "@baseType": "ContactMedium",
             "contactType": "private",
             "id": "c0181f3d83e144a59162fd6136a98462",
             "preferred": true,
             "validFor": {
                "startDateTime": "2018-09-21T23:20:50.52Z"
             },
             "phoneNumber": "+1 202-918-2132"
          },
          "relationDate": "2018-09-21T23:20:50.52Z"
       }
    ],
    "attachment": [
       {
          "@type": "Attachment",
          "attachmentType": "avatarPicture",
          "name": "Neo's avatar",
          "url": "https://i.pravatar.cc/150?u=neo",
          "mimeType": "image/jpeg",
          "size": {
             "amount": 91,
             "units": "Kb"
          },
          "validFor": {
             "startDateTime": "2018-09-21T23:20:50.52Z"
```

```
            }
         }
      ],
      "partyRoleIdentified": [
         {
            "@type": "RelatedSecurityPrincipalRef",
            "role": "Customer",
            "securityPrincipalRef": {
               "href": "https://serverRoot/tmf-
api/customerManagement/v5/partyRole/faa43dccaad142289e2b0f0e73e15958",
               "id": "faa43dccaad142289e2b0f0e73e15958",
               "@type": "PartyRoleRef",
               "@referredType": "PartyRole"
            }
         }
      ],
      "individualIdentified": {
         "href": "https://serverRoot/tmf-
api/partyManagement/v5/individual/193c8d6887394ca5b50290685db512ca",
         "id": "193c8d6887394ca5b50290685db512ca",
         "@type": "IndividualRef",
         "@referredType": "Individual"
      },
      "relatedSecurityPrincipal": [
         {
            "@type": "RelatedSecurityPrincipalRef",
            "role": "ServiceProvider",
            "securityPrincipalRef": {
               "href": "https://serverRoot/tmf-
api/partyManagement/v5/organization/e9b93f395a11453f9b7aa3349e857c24",
               "id": "e9b93f395a11453f9b7aa3349e857c24",
               "@type": "OrganizationRef",
               "@referredType": "Organization",
               "name": "Acme Inc."
            }
         },
         {
            "@type": "RelatedSecurityPrincipalRef",
            "role": "DigitalIdentityProvider",
            "securityPrincipalRef": {
               "href": "https://serverRoot/tmf-
api/partyManagement/v5/organization/af08cfda572749b0b4a90dfb75dfca51",
               "id": "af08cfda572749b0b4a90dfb75dfca51",
               "@type": "OrganizationRef",
               "@referredType": "Organization",
               "name": "Auth0"
            }
         }
      ],
      "creationDate": "2018-09-21T09:13:16-07:00",
      "lastUpdate": "2018-09-21T23:20:50.52Z"
   }
```


## BiometricCredential resource

A Credential based on a login and a password.

### Resource model

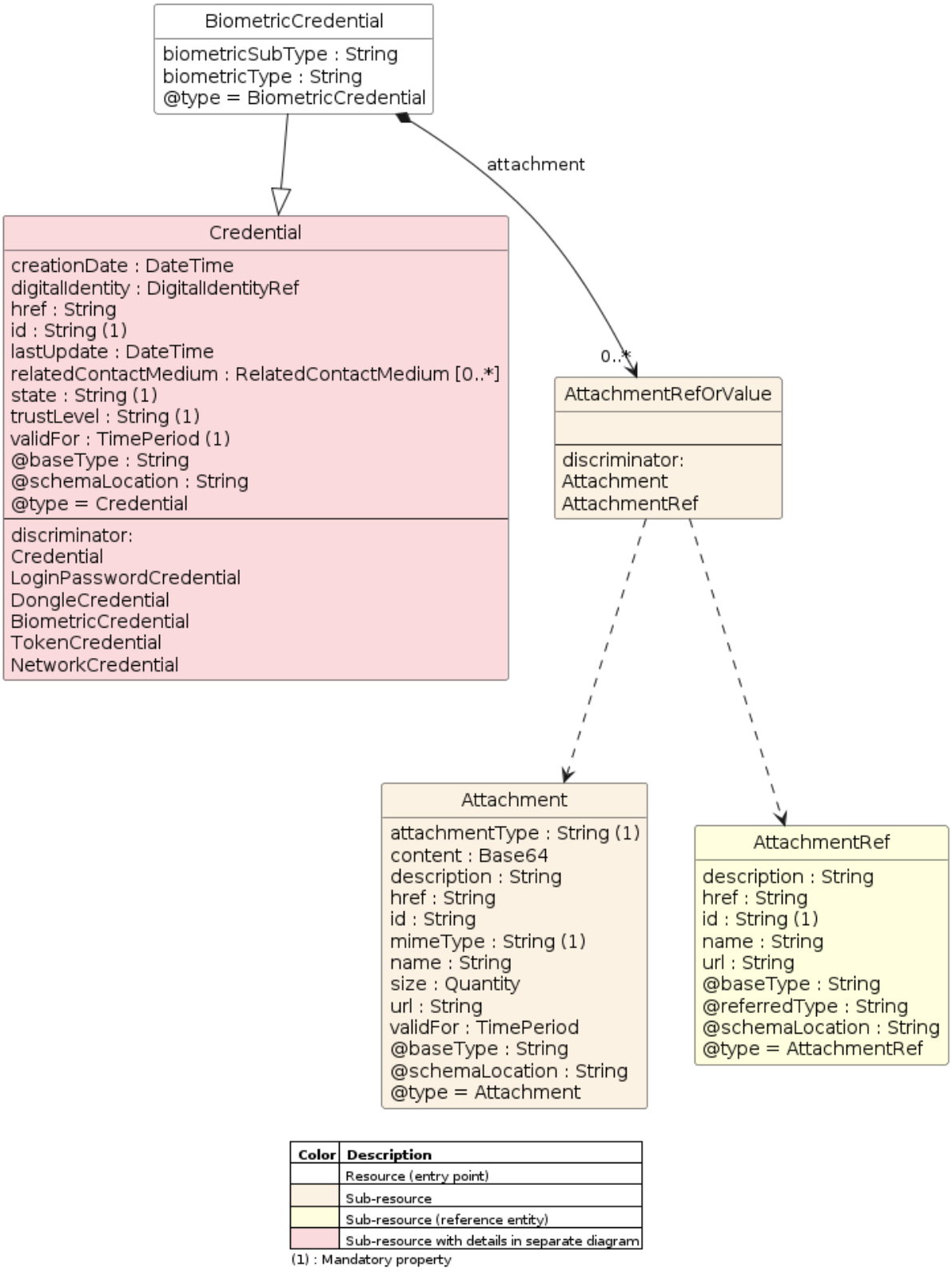


*Figure 3 - BiometricCredential*

## Field descriptions

### BiometricCredential fields

| | |
|---|---|
| attachment | An AttachmentRefOrValue. The polymorphic attributes @type, @schemaLocation & @referredType are related to the Attachment entity and not the AttachmentRefOrValue class itself. |
| biometricSubType | A String. A biometric sub type when required like for finger: thumb, index, ring , pinkyFinger, etc. |
| biometricType | A String. A biometric type like finger, iris, face, etc… |
| creationDate | A DateTime. Date and time of the Credential creation (timestamp). |
| digitalIdentity | A DigitalIdentityRef. DigitalIdentity reference. |
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| lastUpdate | A DateTime. Date and time of the Credential last update (timestamp). |
| relatedContactMedium | A RelatedContactMedium. A ContactMedium and an associated role such as digital-id-recovery-email, digital-id-recovery-phone, digital-id-2nd-factor-email, digital-id-2nd-factor-phone, credential-login-alias-email, credential-login-alias-phone. |
| state | A String. Active (The credential is currently active and can be used for authentication.), Inactive (The credential is inactive and cannot be used for authentication. This status might occur if the user requested to deactivate the credential temporarily), Expired (The credential has passed its expiration date and cannot be used for authentication. Users may need to renew or update their credential to regain access.), Locked (The credential has been temporarily locked due to multiple failed authentication attempts or security policy violations. This status prevents the credential from being used until it's unlocked by an administrator or through a predefined process.), Revoked (The credential has been permanently revoked, usually due to security concerns or policy violations. Once revoked, the credential cannot be used for authentication and may require additional actions to reinstate.) Pending (The credential is awaiting approval or activation. This status is common for newly created credentials that require administrative review or user verification before becoming active.), Suspended )The credential has been temporarily suspended, often due to a security investigation or compliance issue. While suspended, the credential cannot be used for authentication until the suspension is lifted.), Disabled (Similar to inactive, this status indicates that the credential is currently disabled and cannot be used for authentication. However, unlike inactive, disabled status may imply a more permanent state or administrative action.), Unverified (The credential has been created but not yet verified. Users may need to complete additional steps to verify their identity before the credential becomes active.), Compromised (The credential has been compromised or suspected of being compromised. This status is used to indicate potential security breaches, and immediate action is required to mitigate risks, such as resetting the credential or investigating further.). |

| | |
|---|---|
| trustLevel | A String. A level of assurance associated with this credential - this could be used to limit/allow specific permission based on this trust level. |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### Attachment sub-resource fields

| | |
|---|---|
| attachmentType | A String. A business characterization of the purpose of the attachment, for example logo, instructionManual, contractCopy. |
| content | A Base64. The actual contents of the attachment object, if embedded, encoded as base64. |
| description | A String. A narrative text describing the content of the attachment. |
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| mimeType | A String. A technical characterization of the attachment content format using IETF Mime Types. |
| name | A String. The name of the attachment. |
| size | A Quantity. An amount in a given unit. |
| url | A String. Uniform Resource Locator, is a web page address (a subset of URI). |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### AttachmentRef sub-resource fields

| | |
|---|---|
| description | A String. A narrative text describing the content of the attachment. |
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| name | A String. Name of the referred entity. |

| | |
|---|---|
| url | A String. Link to the attachment media/content. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @referredType | A String. The actual type of the target instance when needed for disambiguation. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### Json representation sample(s)

We provide below a JSON representation as example of the 'BiometricCredential' resource object.


```
{
    "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/biometricCredential/754ea8ed4bef49d78ca2ba3f953cd65
f",
    "id": "754ea8ed4bef49d78ca2ba3f953cd65f",
    "@type": "BiometricCredential",
    "@baseType": "Credential",
    "state": "Active",
    "validFor": {
        "startDateTime": "2018-09-21T23:20:50.52Z"
    },
    "trustLevel": "high",
    "biometricType": "finger",
    "biometricSubType": "thumb",
    "attachment": [
        {
            "@type": "Attachment",
            "attachmentType": "thumbFingerprint",
            "name": "Thumb fingerprint",
            "content": "d2VyZndlcmZyd2VyZXJ3Zn...",
            "mimeType": "image/png",
            "size": {
               "amount": 104,
               "units": "Kb"
            },
            "validFor": {
               "startDateTime": "2018-09-21T23:20:50.52Z"
            }
         }
    ],
    "creationDate": "2018-09-21T09:13:16-07:00",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```


## DongleCredential resource

DongleCredential uses a hardware (dongle) that connects to a port on another device to identify / authenticate. In some cases an additional password might be required and checked on the dongle.

### Resource model

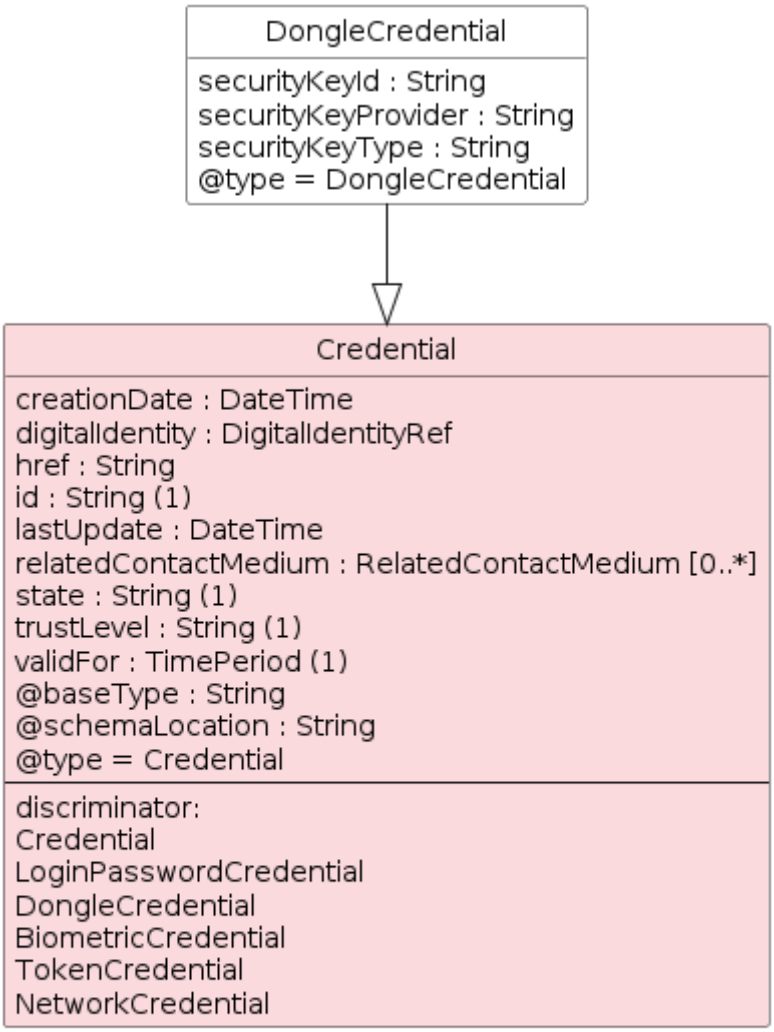


*Figure 4 - DongleCredential*

### Field descriptions

### DongleCredential fields

| | |
|---|---|
| creationDate | A DateTime. Date and time of the Credential creation (timestamp). |
| digitalIdentity | A DigitalIdentityRef. DigitalIdentity reference. |
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |

| | |
|---|---|
| lastUpdate | A DateTime. Date and time of the Credential last update (timestamp). |
| relatedContactMedium | A RelatedContactMedium. A ContactMedium and an associated role such as digital-id-recovery-email, digital-id-recovery-phone, digital-id-2nd-factor-email, digital-id-2nd-factor-phone, credential-login-alias-email, credential-login-alias-phone. |
| securityKeyId | A String. A security key identifier, also known as the credential ID, is a unique identifier associated with a specific security key. It is generated during the enrollment process when a security key is registered with a service or platform. The security key identifier is used to identify and authenticate the security key during subsequent login attempts. It serves as a reference to the corresponding cryptographic key pair stored securely within the security key. |
| securityKeyProvider | A String. A security key provider refers to an entity, such as a manufacturer, vendor, or service provider, that supplies or offers security keys to end-users or organizations. These providers may develop and produce the physical security key devices or provide the associated software, services, and infrastructure necessary for their usage. Security key providers play a crucial role in ensuring the availability, quality, and security of the security keys and associated components, including firmware updates, key management systems, and authentication protocols. They may also offer additional services like customer support, integration assistance, and compliance with industry standards. |
| securityKeyType | A String. The security key type refers to the classification or category of a security key based on its underlying technology or functionality. Examples: USB security key, NFC security key. |

| | |
|---|---|
| state | A String. Active (The credential is currently active and can be used for authentication.), Inactive (The credential is inactive and cannot be used for authentication. This status might occur if the user requested to deactivate the credential temporarily), Expired (The credential has passed its expiration date and cannot be used for authentication. Users may need to renew or update their credential to regain access.), Locked (The credential has been temporarily locked due to multiple failed authentication attempts or security policy violations. This status prevents the credential from being used until it's unlocked by an administrator or through a predefined process.), Revoked (The credential has been permanently revoked, usually due to security concerns or policy violations. Once revoked, the credential cannot be used for authentication and may require additional actions to reinstate.) Pending (The credential is awaiting approval or activation. This status is common for newly created credentials that require administrative review or user verification before becoming active.), Suspended )The credential has been temporarily suspended, often due to a security investigation or compliance issue. While suspended, the credential cannot be used for authentication until the suspension is lifted.), Disabled (Similar to inactive, this status indicates that the credential is currently disabled and cannot be used for authentication. However, unlike inactive, disabled status may imply a more permanent state or administrative action.), Unverified (The credential has been created but not yet verified. Users may need to complete additional steps to verify their identity before the credential becomes active.), Compromised (The credential has been compromised or suspected of being compromised. This status is used to indicate potential security breaches, and immediate action is required to mitigate risks, such as resetting the credential or investigating further.). |
| trustLevel | A String. A level of assurance associated with this credential - this could be used to limit/allow specific permission based on this trust level. |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### Json representation sample(s)

We provide below a JSON representation as example of the 'DongleCredential' resource object.

```
{
    "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/dongleCredential/f4435d1e425a420da6e80abb4c075b22",
    "id": "f4435d1e425a420da6e80abb4c075b22",
```

```
    "@type": "DongleCredential",
    "@baseType": "Credential",
    "state": "Active",
    "validFor": {
        "startDateTime": "2018-09-21T23:20:50.52Z"
    },
    "trustLevel": "high",
    "securityKeyId": "AE7671DF35BD581F467AB9B3DCF92",
    "securityKeyType": "USB Security Key",
    "securityKeyProvider": "Yubico",
    "creationDate": "2018-09-21T09:13:16-07:00",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```


## LoginPasswordCredential resource

A Credential based on a login and a password.

### Resource model

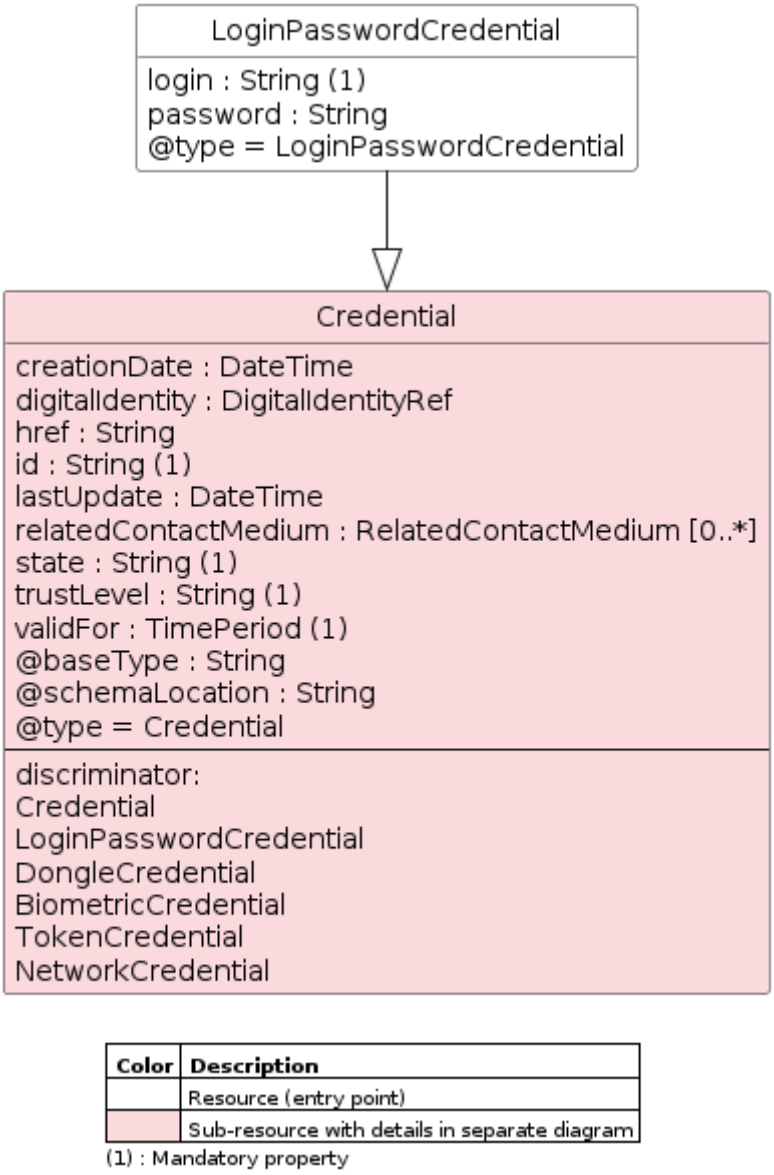


*Figure 5 - LoginPasswordCredential*

## Field descriptions

### LoginPasswordCredential fields

| | |
|---|---|
| creationDate | A DateTime. Date and time of the Credential creation (timestamp). |
| digitalIdentity | A DigitalIdentityRef. DigitalIdentity reference. |
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| lastUpdate | A DateTime. Date and time of the Credential last update (timestamp). |
| login | A String. Credential login. |

| | |
|---|---|
| password | A String. Credential password - must be in write only. |
| relatedContactMedium | A RelatedContactMedium. A ContactMedium and an associated role such as digital-id-recovery-email, digital-id-recovery-phone, digital-id-2nd-factor-email, digital-id-2nd-factor-phone, credential-login-alias-email, credential-login-alias-phone. |
| state | A String. Active (The credential is currently active and can be used for authentication.), Inactive (The credential is inactive and cannot be used for authentication. This status might occur if the user requested to deactivate the credential temporarily), Expired (The credential has passed its expiration date and cannot be used for authentication. Users may need to renew or update their credential to regain access.), Locked (The credential has been temporarily locked due to multiple failed authentication attempts or security policy violations. This status prevents the credential from being used until it's unlocked by an administrator or through a predefined process.), Revoked (The credential has been permanently revoked, usually due to security concerns or policy violations. Once revoked, the credential cannot be used for authentication and may require additional actions to reinstate.) Pending (The credential is awaiting approval or activation. This status is common for newly created credentials that require administrative review or user verification before becoming active.), Suspended )The credential has been temporarily suspended, often due to a security investigation or compliance issue. While suspended, the credential cannot be used for authentication until the suspension is lifted.), Disabled (Similar to inactive, this status indicates that the credential is currently disabled and cannot be used for authentication. However, unlike inactive, disabled status may imply a more permanent state or administrative action.), Unverified (The credential has been created but not yet verified. Users may need to complete additional steps to verify their identity before the credential becomes active.), Compromised (The credential has been compromised or suspected of being compromised. This status is used to indicate potential security breaches, and immediate action is required to mitigate risks, such as resetting the credential or investigating further.). |
| trustLevel | A String. A level of assurance associated with this credential - this could be used to limit/allow specific permission based on this trust level. |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### Json representation sample(s)

We provide below a JSON representation as example of the 'LoginPasswordCredential'

resource object.


```
{
    "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/loginPasswordCredential/41af4b86e0b144cb9099b3d4c3a
b26ae",
    "id": "41af4b86e0b144cb9099b3d4c3ab26ae",
    "@type": "LoginPasswordCredential",
    "@baseType": "Credential",
    "state": "Active",
    "validFor": {
       "startDateTime": "2018-09-21T23:20:50.52Z"
    },
    "trustLevel": "high",
    "relatedContactMedium": [
       {
          "@type": "RelatedContactMedium",
          "role": "credential-login-alias-email",
          "contactMedium": {
             "@type": "EmailContactMedium",
             "@baseType": "ContactMedium",
             "contactType": "private",
             "id": "b2fe04a7f96e479195a47710abcf72be",
             "preferred": true,
             "validFor": {
                "startDateTime": "2018-09-21T23:20:50.52Z"
             },
             "verified": true,
             "emailAddress": "neo@matrix.com"
          },
          "relationDate": "2018-09-21T23:20:50.52Z"
       },
       {
          "@type": "RelatedContactMedium",
          "role": "credential-login-alias-phone",
          "contactMedium": {
             "@type": "PhoneContactMedium",
             "@baseType": "ContactMedium",
             "contactType": "private",
             "id": "c0181f3d83e144a59162fd6136a98462",
             "preferred": true,
             "validFor": {
                "startDateTime": "2018-09-21T23:20:50.52Z"
             },
             "verified": true,
             "phoneNumber": "+1 202-918-2132"
          },
          "relationDate": "2018-09-21T23:20:50.52Z"
       }
    ],
    "login": "neo1999",
    "creationDate": "2018-09-21T09:13:16-07:00",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
 }
```


## NetworkCredential resource

A Credential based on a login and a password.

### Resource model

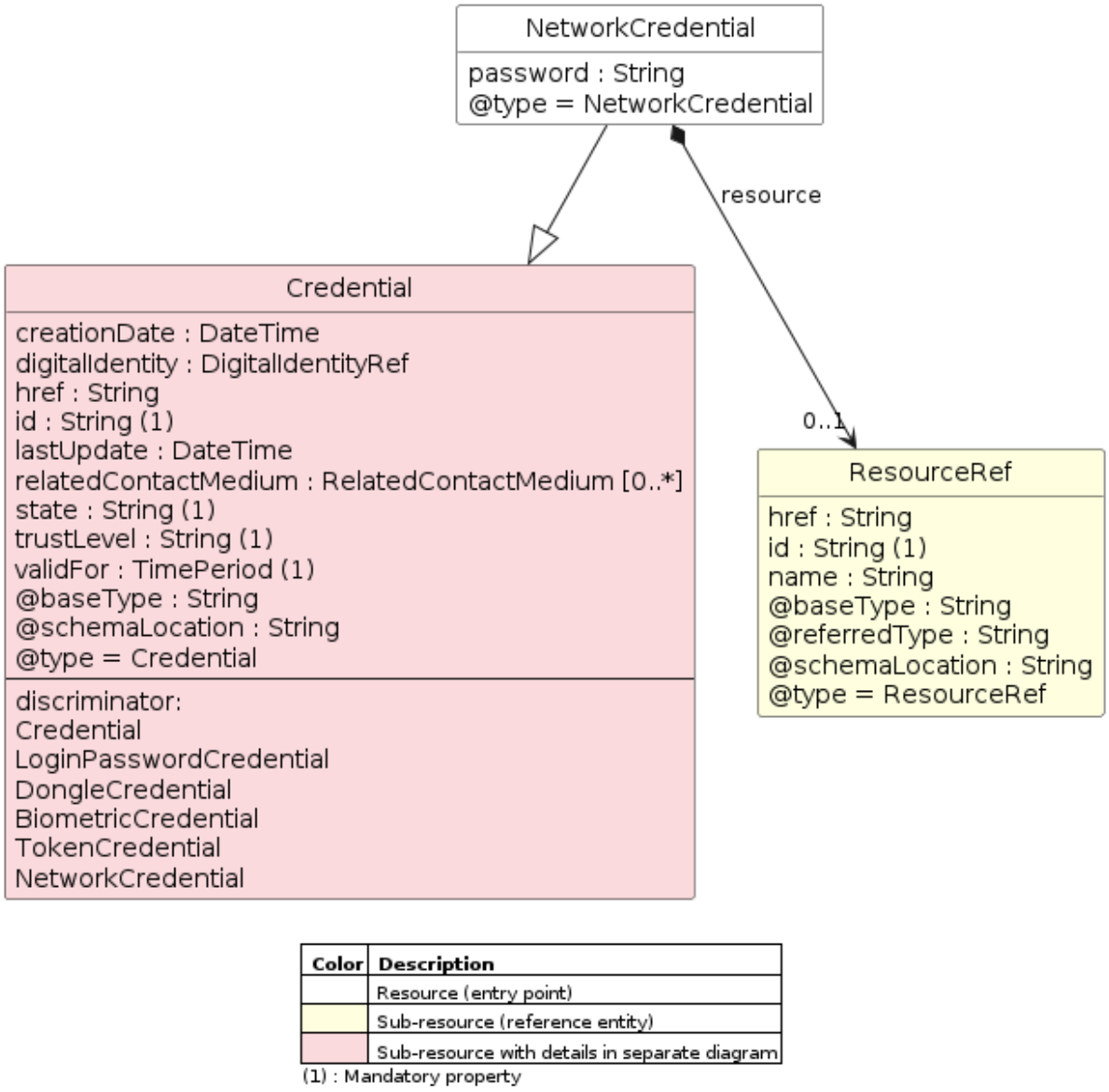


*Figure 6 - NetworkCredential*

### Field descriptions

### NetworkCredential fields

| | |
|---|---|
| creationDate | A DateTime. Date and time of the Credential creation (timestamp). |
| digitalIdentity | A DigitalIdentityRef. DigitalIdentity reference. |
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| lastUpdate | A DateTime. Date and time of the Credential last update (timestamp). |

| | |
|---|---|
| password | A String. Credential password to use resource based credential. Sensitive data such as passwords MUST be ommitted in GET responses. |
| relatedContactMedium | A RelatedContactMedium. A ContactMedium and an associated role such as digital-id-recovery-email, digital-id-recovery-phone, digital-id-2nd-factor-email, digital-id-2nd-factor-phone, credential-login-alias-email, credential-login-alias-phone. |
| resource | A ResourceRef. Resource reference, for when Resource is used by other entities. |
| state | A String. Active (The credential is currently active and can be used for authentication.), Inactive (The credential is inactive and cannot be used for authentication. This status might occur if the user requested to deactivate the credential temporarily), Expired (The credential has passed its expiration date and cannot be used for authentication. Users may need to renew or update their credential to regain access.), Locked (The credential has been temporarily locked due to multiple failed authentication attempts or security policy violations. This status prevents the credential from being used until it's unlocked by an administrator or through a predefined process.), Revoked (The credential has been permanently revoked, usually due to security concerns or policy violations. Once revoked, the credential cannot be used for authentication and may require additional actions to reinstate.) Pending (The credential is awaiting approval or activation. This status is common for newly created credentials that require administrative review or user verification before becoming active.), Suspended )The credential has been temporarily suspended, often due to a security investigation or compliance issue. While suspended, the credential cannot be used for authentication until the suspension is lifted.), Disabled (Similar to inactive, this status indicates that the credential is currently disabled and cannot be used for authentication. However, unlike inactive, disabled status may imply a more permanent state or administrative action.), Unverified (The credential has been created but not yet verified. Users may need to complete additional steps to verify their identity before the credential becomes active.), Compromised (The credential has been compromised or suspected of being compromised. This status is used to indicate potential security breaches, and immediate action is required to mitigate risks, such as resetting the credential or investigating further.). |
| trustLevel | A String. A level of assurance associated with this credential - this could be used to limit/allow specific permission based on this trust level. |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### ResourceRef sub-resource fields

| | |
|---|---|
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| name | A String. Name of the referred entity. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @referredType | A String. The actual type of the target instance when needed for disambiguation. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### Json representation sample(s)

We provide below a JSON representation as example of the 'NetworkCredential' resource object.


```
{
    "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/networkCredential/9fd97c82b4bf4fe7bcbee314d811290b"
,
    "id": "9fd97c82b4bf4fe7bcbee314d811290b",
    "@type": "NetworkCredential",
    "@baseType": "Credential",
    "state": "Active",
    "validFor": {
        "startDateTime": "2018-09-21T23:20:50.52Z"
    },
    "trustLevel": "high",
    "resource": {
        "@type": "ResourceRef",
        "id": "99729be76fa948d5a1df22618bec96ea"
    },
    "creationDate": "2018-09-21T09:13:16-07:00",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```


## TokenCredential resource

A Credential based on a token.

### Resource model

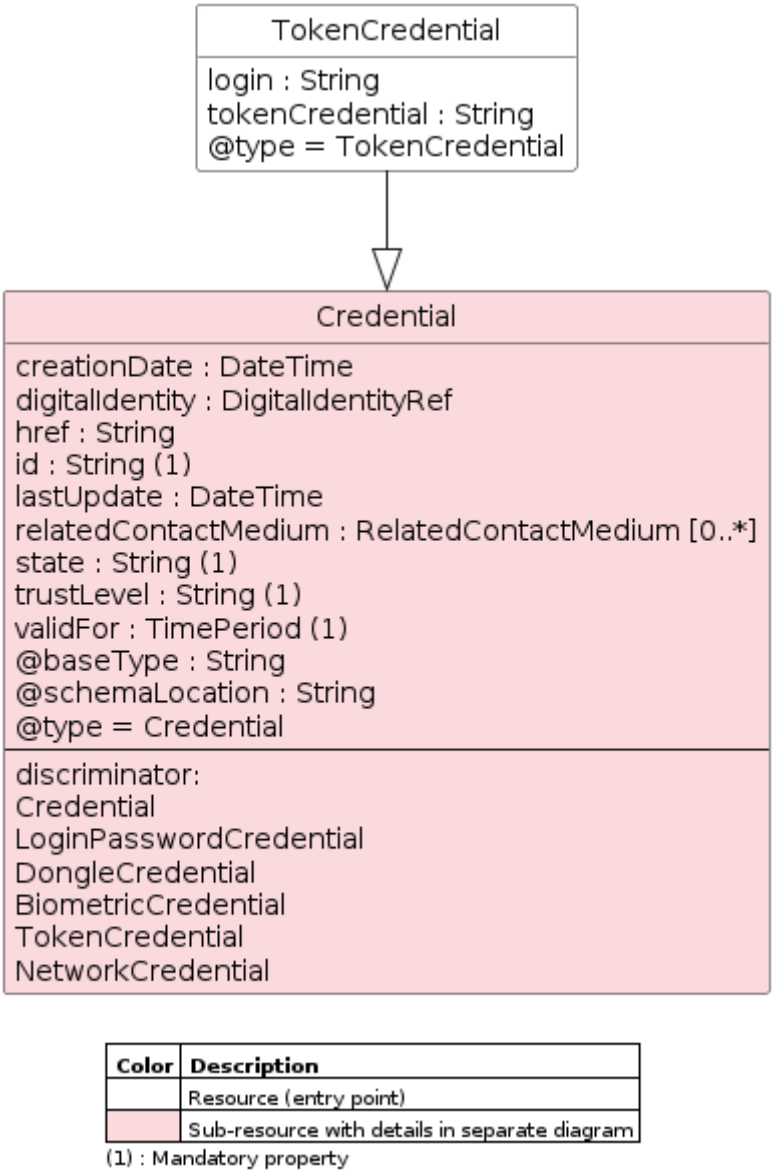


*Figure 7 - TokenCredential*

## Field descriptions

### TokenCredential fields

| | |
|---|---|
| creationDate | A DateTime. Date and time of the Credential creation (timestamp). |
| digitalIdentity | A DigitalIdentityRef. DigitalIdentity reference. |
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| lastUpdate | A DateTime. Date and time of the Credential last update (timestamp). |
| login | A String. Credential login. |

| | |
|---|---|
| relatedContactMedium | A RelatedContactMedium. A ContactMedium and an associated role such as digital-id-recovery-email, digital-id-recovery-phone, digital-id-2nd-factor-email, digital-id-2nd-factor-phone, credential-login-alias-email, credential-login-alias-phone. |
| state | A String. Active (The credential is currently active and can be used for authentication.), Inactive (The credential is inactive and cannot be used for authentication. This status might occur if the user requested to deactivate the credential temporarily), Expired (The credential has passed its expiration date and cannot be used for authentication. Users may need to renew or update their credential to regain access.), Locked (The credential has been temporarily locked due to multiple failed authentication attempts or security policy violations. This status prevents the credential from being used until it's unlocked by an administrator or through a predefined process.), Revoked (The credential has been permanently revoked, usually due to security concerns or policy violations. Once revoked, the credential cannot be used for authentication and may require additional actions to reinstate.) Pending (The credential is awaiting approval or activation. This status is common for newly created credentials that require administrative review or user verification before becoming active.), Suspended )The credential has been temporarily suspended, often due to a security investigation or compliance issue. While suspended, the credential cannot be used for authentication until the suspension is lifted.), Disabled (Similar to inactive, this status indicates that the credential is currently disabled and cannot be used for authentication. However, unlike inactive, disabled status may imply a more permanent state or administrative action.), Unverified (The credential has been created but not yet verified. Users may need to complete additional steps to verify their identity before the credential becomes active.), Compromised (The credential has been compromised or suspected of being compromised. This status is used to indicate potential security breaches, and immediate action is required to mitigate risks, such as resetting the credential or investigating further.). |
| tokenCredential | A String. Token credential identifier. |
| trustLevel | A String. A level of assurance associated with this credential - this could be used to limit/allow specific permission based on this trust level. |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### Json representation sample(s)

We provide below a JSON representation as example of the 'TokenCredential' resource

object.


```
{
    "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/tokenCredential/7ef64b30fd5345ac9ab9554798c21f5c",
    "id": "7ef64b30fd5345ac9ab9554798c21f5c",
    "@type": "TokenCredential",
    "@baseType": "Credential",
    "state": "Active",
    "validFor": {
       "startDateTime": "2018-09-21T23:20:50.52Z",
       "endDateTime": "2018-10-21T23:20:50.52Z"
    },
    "trustLevel": "high",
    "login": "google.id:107691503500061507151130823 67",
    "tokenCredential":
"6nxugrzcv0e4se81kufqf0nn0rpygf4yqzyp7gha68wgqdpm057lx97jiiy6fdpq",
    "creationDate": "2018-09-21T09:13:16-07:00",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
 }
```


## CheckCredential resource

The CheckCredential task entity checks if credential is valid.

### Resource model

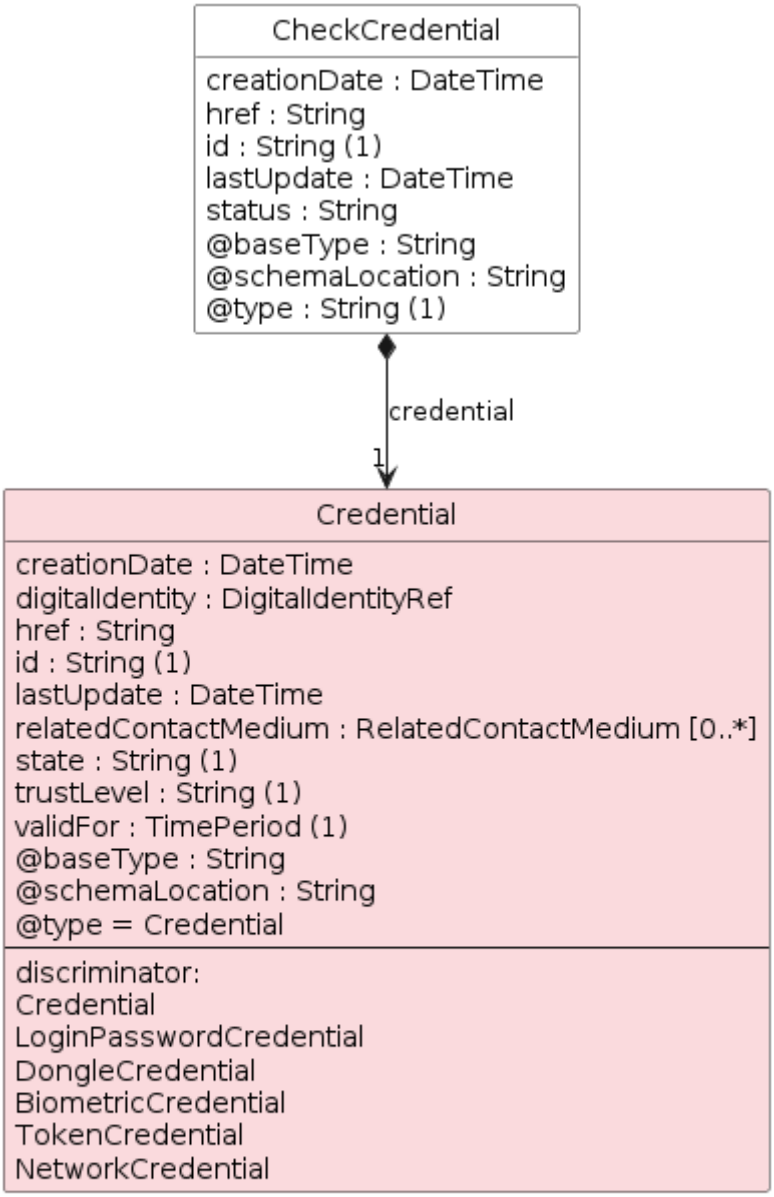


*Figure 8 - CheckCredential*

### Field descriptions

### CheckCredential fields

| | |
|---|---|
| creationDate | A DateTime. Date at which the CheckCredential task resource was created. |

| | |
|---|---|
| credential | A Credential. A Credential is a pure-virtual super-class that defines a specific credential such as Biometric Credential, Dongle Credential, Login Password Credential, Network Credential and Token Credential with all details associated. Use the @type attribute to specify the concrete type in the API calls.<br><br>Credential can be instanciated as<br>* BiometricCredential<br>* DongleCredential<br>* LoginPasswordCredential<br>* NetworkCredential<br>* TokenCredential |
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| lastUpdate | A DateTime. Date and time of the Credential last update (timestamp). |
| status | A String. Pending, running, succeded, failed. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### Credential sub-resource fields

| | |
|---|---|
| creationDate | A DateTime. Date and time of the Credential creation (timestamp). |
| digitalIdentity | A DigitalIdentityRef. DigitalIdentity reference. |
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| lastUpdate | A DateTime. Date and time of the Credential last update (timestamp). |
| relatedContactMedium | A RelatedContactMedium. A ContactMedium and an associated role such as digital-id-recovery-email, digital-id-recovery-phone, digital-id-2nd-factor-email, digital-id-2nd-factor-phone, credential-login-alias-email, credential-login-alias-phone. |

| | |
|---|---|
| state | A String. Active (The credential is currently active and can be used for authentication.), Inactive (The credential is inactive and cannot be used for authentication. This status might occur if the user requested to deactivate the credential temporarily), Expired (The credential has passed its expiration date and cannot be used for authentication. Users may need to renew or update their credential to regain access.), Locked (The credential has been temporarily locked due to multiple failed authentication attempts or security policy violations. This status prevents the credential from being used until it's unlocked by an administrator or through a predefined process.), Revoked (The credential has been permanently revoked, usually due to security concerns or policy violations. Once revoked, the credential cannot be used for authentication and may require additional actions to reinstate.) Pending (The credential is awaiting approval or activation. This status is common for newly created credentials that require administrative review or user verification before becoming active.), Suspended )The credential has been temporarily suspended, often due to a security investigation or compliance issue. While suspended, the credential cannot be used for authentication until the suspension is lifted.), Disabled (Similar to inactive, this status indicates that the credential is currently disabled and cannot be used for authentication. However, unlike inactive, disabled status may imply a more permanent state or administrative action.), Unverified (The credential has been created but not yet verified. Users may need to complete additional steps to verify their identity before the credential becomes active.), Compromised (The credential has been compromised or suspected of being compromised. This status is used to indicate potential security breaches, and immediate action is required to mitigate risks, such as resetting the credential or investigating further.). |
| trustLevel | A String. A level of assurance associated with this credential - this could be used to limit/allow specific permission based on this trust level. |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |
| | Credential can be instanciated as<br>* BiometricCredential<br>* DongleCredential<br>* LoginPasswordCredential<br>* NetworkCredential<br>* TokenCredential |
| attachment | This property is present in subclasses |
| biometricSubType | This property is present in subclasses |

| | |
|---|---|
| biometricType | This property is present in subclasses |
| login | This property is present in subclasses |
| password | This property is present in subclasses |
| resource | This property is present in subclasses |
| securityKeyId | This property is present in subclasses |
| securityKeyProvider | This property is present in subclasses |
| securityKeyType | This property is present in subclasses |
| tokenCredential | This property is present in subclasses |

### LoginPasswordCredential sub-resource fields

| | |
|---|---|
| creationDate | A DateTime. Date and time of the Credential creation (timestamp). |
| digitalIdentity | A DigitalIdentityRef. DigitalIdentity reference. |
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| lastUpdate | A DateTime. Date and time of the Credential last update (timestamp). |
| login | A String. Credential login. |
| password | A String. Credential password - must be in write only. |
| relatedContactMedium | A RelatedContactMedium. A ContactMedium and an associated role such as digital-id-recovery-email, digital-id-recovery-phone, digital-id-2nd-factor-email, digital-id-2nd-factor-phone, credential-login-alias-email, credential-login-alias-phone. |

| | |
|---|---|
| state | A String. Active (The credential is currently active and can be used for authentication.), Inactive (The credential is inactive and cannot be used for authentication. This status might occur if the user requested to deactivate the credential temporarily), Expired (The credential has passed its expiration date and cannot be used for authentication. Users may need to renew or update their credential to regain access.), Locked (The credential has been temporarily locked due to multiple failed authentication attempts or security policy violations. This status prevents the credential from being used until it's unlocked by an administrator or through a predefined process.), Revoked (The credential has been permanently revoked, usually due to security concerns or policy violations. Once revoked, the credential cannot be used for authentication and may require additional actions to reinstate.) Pending (The credential is awaiting approval or activation. This status is common for newly created credentials that require administrative review or user verification before becoming active.), Suspended )The credential has been temporarily suspended, often due to a security investigation or compliance issue. While suspended, the credential cannot be used for authentication until the suspension is lifted.), Disabled (Similar to inactive, this status indicates that the credential is currently disabled and cannot be used for authentication. However, unlike inactive, disabled status may imply a more permanent state or administrative action.), Unverified (The credential has been created but not yet verified. Users may need to complete additional steps to verify their identity before the credential becomes active.), Compromised (The credential has been compromised or suspected of being compromised. This status is used to indicate potential security breaches, and immediate action is required to mitigate risks, such as resetting the credential or investigating further.). |
| trustLevel | A String. A level of assurance associated with this credential - this could be used to limit/allow specific permission based on this trust level. |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### DongleCredential sub-resource fields

| | |
|---|---|
| creationDate | A DateTime. Date and time of the Credential creation (timestamp). |
| digitalIdentity | A DigitalIdentityRef. DigitalIdentity reference. |
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |

| | |
|---|---|
| lastUpdate | A DateTime. Date and time of the Credential last update (timestamp). |
| relatedContactMedium | A RelatedContactMedium. A ContactMedium and an associated role such as digital-id-recovery-email, digital-id-recovery-phone, digital-id-2nd-factor-email, digital-id-2nd-factor-phone, credential-login-alias-email, credential-login-alias-phone. |
| securityKeyId | A String. A security key identifier, also known as the credential ID, is a unique identifier associated with a specific security key. It is generated during the enrollment process when a security key is registered with a service or platform. The security key identifier is used to identify and authenticate the security key during subsequent login attempts. It serves as a reference to the corresponding cryptographic key pair stored securely within the security key. |
| securityKeyProvider | A String. A security key provider refers to an entity, such as a manufacturer, vendor, or service provider, that supplies or offers security keys to end-users or organizations. These providers may develop and produce the physical security key devices or provide the associated software, services, and infrastructure necessary for their usage. Security key providers play a crucial role in ensuring the availability, quality, and security of the security keys and associated components, including firmware updates, key management systems, and authentication protocols. They may also offer additional services like customer support, integration assistance, and compliance with industry standards. |
| securityKeyType | A String. The security key type refers to the classification or category of a security key based on its underlying technology or functionality. Examples: USB security key, NFC security key. |

| | |
|---|---|
| state | A String. Active (The credential is currently active and can be used for authentication.), Inactive (The credential is inactive and cannot be used for authentication. This status might occur if the user requested to deactivate the credential temporarily), Expired (The credential has passed its expiration date and cannot be used for authentication. Users may need to renew or update their credential to regain access.), Locked (The credential has been temporarily locked due to multiple failed authentication attempts or security policy violations. This status prevents the credential from being used until it's unlocked by an administrator or through a predefined process.), Revoked (The credential has been permanently revoked, usually due to security concerns or policy violations. Once revoked, the credential cannot be used for authentication and may require additional actions to reinstate.) Pending (The credential is awaiting approval or activation. This status is common for newly created credentials that require administrative review or user verification before becoming active.), Suspended )The credential has been temporarily suspended, often due to a security investigation or compliance issue. While suspended, the credential cannot be used for authentication until the suspension is lifted.), Disabled (Similar to inactive, this status indicates that the credential is currently disabled and cannot be used for authentication. However, unlike inactive, disabled status may imply a more permanent state or administrative action.), Unverified (The credential has been created but not yet verified. Users may need to complete additional steps to verify their identity before the credential becomes active.), Compromised (The credential has been compromised or suspected of being compromised. This status is used to indicate potential security breaches, and immediate action is required to mitigate risks, such as resetting the credential or investigating further.). |
| trustLevel | A String. A level of assurance associated with this credential - this could be used to limit/allow specific permission based on this trust level. |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### BiometricCredential sub-resource fields

| | |
|---|---|
| attachment | An AttachmentRefOrValue. The polymorphic attributes @type, @schemaLocation & @referredType are related to the Attachment entity and not the AttachmentRefOrValue class itself. |
| biometricSubType | A String. A biometric sub type when required like for finger: thumb, index, ring , pinkyFinger, etc. |
| biometricType | A String. A biometric type like finger, iris, face, etc… |

| | |
|---|---|
| creationDate | A DateTime. Date and time of the Credential creation (timestamp). |
| digitalIdentity | A DigitalIdentityRef. DigitalIdentity reference. |
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| lastUpdate | A DateTime. Date and time of the Credential last update (timestamp). |
| relatedContactMedium | A RelatedContactMedium. A ContactMedium and an associated role such as digital-id-recovery-email, digital-id-recovery-phone, digital-id-2nd-factor-email, digital-id-2nd-factor-phone, credential-login-alias-email, credential-login-alias-phone. |
| state | A String. Active (The credential is currently active and can be used for authentication.), Inactive (The credential is inactive and cannot be used for authentication. This status might occur if the user requested to deactivate the credential temporarily), Expired (The credential has passed its expiration date and cannot be used for authentication. Users may need to renew or update their credential to regain access.), Locked (The credential has been temporarily locked due to multiple failed authentication attempts or security policy violations. This status prevents the credential from being used until it's unlocked by an administrator or through a predefined process.), Revoked (The credential has been permanently revoked, usually due to security concerns or policy violations. Once revoked, the credential cannot be used for authentication and may require additional actions to reinstate.) Pending (The credential is awaiting approval or activation. This status is common for newly created credentials that require administrative review or user verification before becoming active.), Suspended )The credential has been temporarily suspended, often due to a security investigation or compliance issue. While suspended, the credential cannot be used for authentication until the suspension is lifted.), Disabled (Similar to inactive, this status indicates that the credential is currently disabled and cannot be used for authentication. However, unlike inactive, disabled status may imply a more permanent state or administrative action.), Unverified (The credential has been created but not yet verified. Users may need to complete additional steps to verify their identity before the credential becomes active.), Compromised (The credential has been compromised or suspected of being compromised. This status is used to indicate potential security breaches, and immediate action is required to mitigate risks, such as resetting the credential or investigating further.). |
| trustLevel | A String. A level of assurance associated with this credential - this could be used to limit/allow specific permission based on this trust level. |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |

| | |
|---|---|
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### TokenCredential sub-resource fields

| | |
|---|---|
| creationDate | A DateTime. Date and time of the Credential creation (timestamp). |
| digitalIdentity | A DigitalIdentityRef. DigitalIdentity reference. |
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| lastUpdate | A DateTime. Date and time of the Credential last update (timestamp). |
| login | A String. Credential login. |
| relatedContactMedium | A RelatedContactMedium. A ContactMedium and an associated role such as digital-id-recovery-email, digital-id-recovery-phone, digital-id-2nd-factor-email, digital-id-2nd-factor-phone, credential-login-alias-email, credential-login-alias-phone. |

| | |
|---|---|
| state | A String. Active (The credential is currently active and can be used for authentication.), Inactive (The credential is inactive and cannot be used for authentication. This status might occur if the user requested to deactivate the credential temporarily), Expired (The credential has passed its expiration date and cannot be used for authentication. Users may need to renew or update their credential to regain access.), Locked (The credential has been temporarily locked due to multiple failed authentication attempts or security policy violations. This status prevents the credential from being used until it's unlocked by an administrator or through a predefined process.), Revoked (The credential has been permanently revoked, usually due to security concerns or policy violations. Once revoked, the credential cannot be used for authentication and may require additional actions to reinstate.) Pending (The credential is awaiting approval or activation. This status is common for newly created credentials that require administrative review or user verification before becoming active.), Suspended )The credential has been temporarily suspended, often due to a security investigation or compliance issue. While suspended, the credential cannot be used for authentication until the suspension is lifted.), Disabled (Similar to inactive, this status indicates that the credential is currently disabled and cannot be used for authentication. However, unlike inactive, disabled status may imply a more permanent state or administrative action.), Unverified (The credential has been created but not yet verified. Users may need to complete additional steps to verify their identity before the credential becomes active.), Compromised (The credential has been compromised or suspected of being compromised. This status is used to indicate potential security breaches, and immediate action is required to mitigate risks, such as resetting the credential or investigating further.). |
| tokenCredential | A String. Token credential identifier. |
| trustLevel | A String. A level of assurance associated with this credential - this could be used to limit/allow specific permission based on this trust level. |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### NetworkCredential sub-resource fields

| | |
|---|---|
| creationDate | A DateTime. Date and time of the Credential creation (timestamp). |
| digitalIdentity | A DigitalIdentityRef. DigitalIdentity reference. |
| href | A String. Hyperlink reference. |

| | |
|---|---|
| id | A String. Unique identifier. |
| lastUpdate | A DateTime. Date and time of the Credential last update (timestamp). |
| password | A String. Credential password to use resource based credential. Sensitive data such as passwords MUST be ommitted in GET responses. |
| relatedContactMedium | A RelatedContactMedium. A ContactMedium and an associated role such as digital-id-recovery-email, digital-id-recovery-phone, digital-id-2nd-factor-email, digital-id-2nd-factor-phone, credential-login-alias-email, credential-login-alias-phone. |
| resource | A ResourceRef. Resource reference, for when Resource is used by other entities. |
| state | A String. Active (The credential is currently active and can be used for authentication.), Inactive (The credential is inactive and cannot be used for authentication. This status might occur if the user requested to deactivate the credential temporarily), Expired (The credential has passed its expiration date and cannot be used for authentication. Users may need to renew or update their credential to regain access.), Locked (The credential has been temporarily locked due to multiple failed authentication attempts or security policy violations. This status prevents the credential from being used until it's unlocked by an administrator or through a predefined process.), Revoked (The credential has been permanently revoked, usually due to security concerns or policy violations. Once revoked, the credential cannot be used for authentication and may require additional actions to reinstate.) Pending (The credential is awaiting approval or activation. This status is common for newly created credentials that require administrative review or user verification before becoming active.), Suspended )The credential has been temporarily suspended, often due to a security investigation or compliance issue. While suspended, the credential cannot be used for authentication until the suspension is lifted.), Disabled (Similar to inactive, this status indicates that the credential is currently disabled and cannot be used for authentication. However, unlike inactive, disabled status may imply a more permanent state or administrative action.), Unverified (The credential has been created but not yet verified. Users may need to complete additional steps to verify their identity before the credential becomes active.), Compromised (The credential has been compromised or suspected of being compromised. This status is used to indicate potential security breaches, and immediate action is required to mitigate risks, such as resetting the credential or investigating further.). |
| trustLevel | A String. A level of assurance associated with this credential - this could be used to limit/allow specific permission based on this trust level. |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |

| | |
|---|---|
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### RelatedContactMedium sub-resource fields

| | |
|---|---|
| contactMedium | A ContactMedium. Indicates the contact medium that could be used to contact the party. This is an abstract base class, the actual value is in one of the strongly-typed subclasses : EmailContactMedium, FaxContactMedium, PhoneContactMedium, GeographicAddressContactMedium, SocialMediaContactMedium…<br><br>ContactMedium can be instanciated as<br>* EmailContactMedium<br>* GeographicAddressContactMedium<br>* PhoneContactMedium |
| relationDate | A DateTime. Date and time when related contact medium was created. |
| role | A String. Role played by related contact medium. E.g: digital-id-recovery-email, digital-id-recovery-phone, digital-id-2nd-factor-email, digital-id-2nd-factor-phone, credential-login-alias-email, credential-login-alias-phone. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### DigitalIdentityRef sub-resource fields

| | |
|---|---|
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| name | A String. Name of the referred entity. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @referredType | A String. The actual type of the target instance when needed for disambiguation. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### ContactMedium sub-resource fields

| | |
|---|---|
| contactType | A String. Type of the contact medium to qualify it like pro email / personal email. This is not used to define the contact medium used. |
| id | A String. Identifier for this contact medium. |
| preferred | A Boolean. If true, indicates that is the preferred contact medium. |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |
| | ContactMedium can be instanciated as<br>* EmailContactMedium<br>* GeographicAddressContactMedium<br>* PhoneContactMedium |
| city | This property is present in subclasses |
| country | This property is present in subclasses |
| emailAddress | This property is present in subclasses |
| geographicAddress | This property is present in subclasses |
| phoneNumber | This property is present in subclasses |
| postCode | This property is present in subclasses |
| stateOrProvince | This property is present in subclasses |
| street1 | This property is present in subclasses |
| street2 | This property is present in subclasses |

### PhoneContactMedium sub-resource fields

| | |
|---|---|
| contactType | A String. Type of the contact medium to qualify it like pro email / personal email. This is not used to define the contact medium used. |
| id | A String. Identifier for this contact medium. |
| phoneNumber | A String. The phone number of the contact. |
| preferred | A Boolean. If true, indicates that is the preferred contact medium. |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### GeographicAddressContactMedium sub-resource fields

| | |
|---|---|
| city | A String. The city. |
| contactType | A String. Type of the contact medium to qualify it like pro email / personal email. This is not used to define the contact medium used. |
| country | A String. The country. |
| geographicAddress | A GeographicAddressRef. Reference to a Geographic Address. |
| id | A String. Identifier for this contact medium. |
| postCode | A String. Postcode. |
| preferred | A Boolean. If true, indicates that is the preferred contact medium. |
| stateOrProvince | A String. State or province. |
| street1 | A String. Describes the street. |
| street2 | A String. Complementary street description. |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### EmailContactMedium sub-resource fields

| | |
|---|---|
| contactType | A String. Type of the contact medium to qualify it like pro email / personal email. This is not used to define the contact medium used. |
| emailAddress | A String. Full email address in standard format. |
| id | A String. Identifier for this contact medium. |
| preferred | A Boolean. If true, indicates that is the preferred contact medium. |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### GeographicAddressRef sub-resource fields

| | |
|---|---|
| href | A String. Hyperlink reference. |

| | |
|---|---|
| id | A String. Unique identifier. |
| name | A String. Name of the referred entity. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @referredType | A String. The actual type of the target instance when needed for disambiguation. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### Attachment sub-resource fields

| | |
|---|---|
| attachmentType | A String. A business characterization of the purpose of the attachment, for example logo, instructionManual, contractCopy. |
| content | A Base64. The actual contents of the attachment object, if embedded, encoded as base64. |
| description | A String. A narrative text describing the content of the attachment. |
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| mimeType | A String. A technical characterization of the attachment content format using IETF Mime Types. |
| name | A String. The name of the attachment. |
| size | A Quantity. An amount in a given unit. |
| url | A String. Uniform Resource Locator, is a web page address (a subset of URI). |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### AttachmentRef sub-resource fields

| | |
|---|---|
| description | A String. A narrative text describing the content of the attachment. |
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| name | A String. Name of the referred entity. |
| url | A String. Link to the attachment media/content. |

| | |
|---|---|
| @baseType | A String. When sub-classing, this defines the super-class. |
| @referredType | A String. The actual type of the target instance when needed for disambiguation. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### ResourceRef sub-resource fields

| | |
|---|---|
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| name | A String. Name of the referred entity. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @referredType | A String. The actual type of the target instance when needed for disambiguation. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### Json representation sample(s)

We provide below a JSON representation as example of the 'CheckCredential' resource object.


```
{
   "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/checkCredential/bf0fc07cff1946079548b7edb0d0db05",
   "id": "bf0fc07cff1946079548b7edb0d0db05",
   "@type": "CheckCredential",
   "credential": {
      "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/loginPasswordCredential/41af4b86e0b144cb9099b3d4c3a
b26ae",
      "id": "41af4b86e0b144cb9099b3d4c3ab26ae",
      "@type": "LoginPasswordCredential",
      "@baseType": "Credential",
      "state": "Active",
      "validFor": {
         "startDateTime": "2018-09-21T23:20:50.52Z"
      },
      "trustLevel": "high",
      "login": "neo1999",
      "digitalIdentity": {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/digitalIdentity/2391ee4acbc142b1a4b74b4d4ab38152",
         "id": "2391ee4acbc142b1a4b74b4d4ab38152",
         "@type": "DigitalIdentityRef",
         "@referredType": "DigitalIdentity"
      },
```

```
        "creationDate": "2018-09-21T09:13:16-07:00",
        "lastUpdate": "2018-09-21T23:20:50.52Z"
    },
    "creationDate": "2018-09-21T09:13:16-07:00",
    "status": "succeded",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```


## Credential resource

A Credential is a pure-virtual super-class that defines a specific credential such as Biometric Credential, Dongle Credential, Login Password Credential, Network Credential and Token Credential with all details associated. Use the @type attribute to specify the concrete type in the API calls.

### Resource model

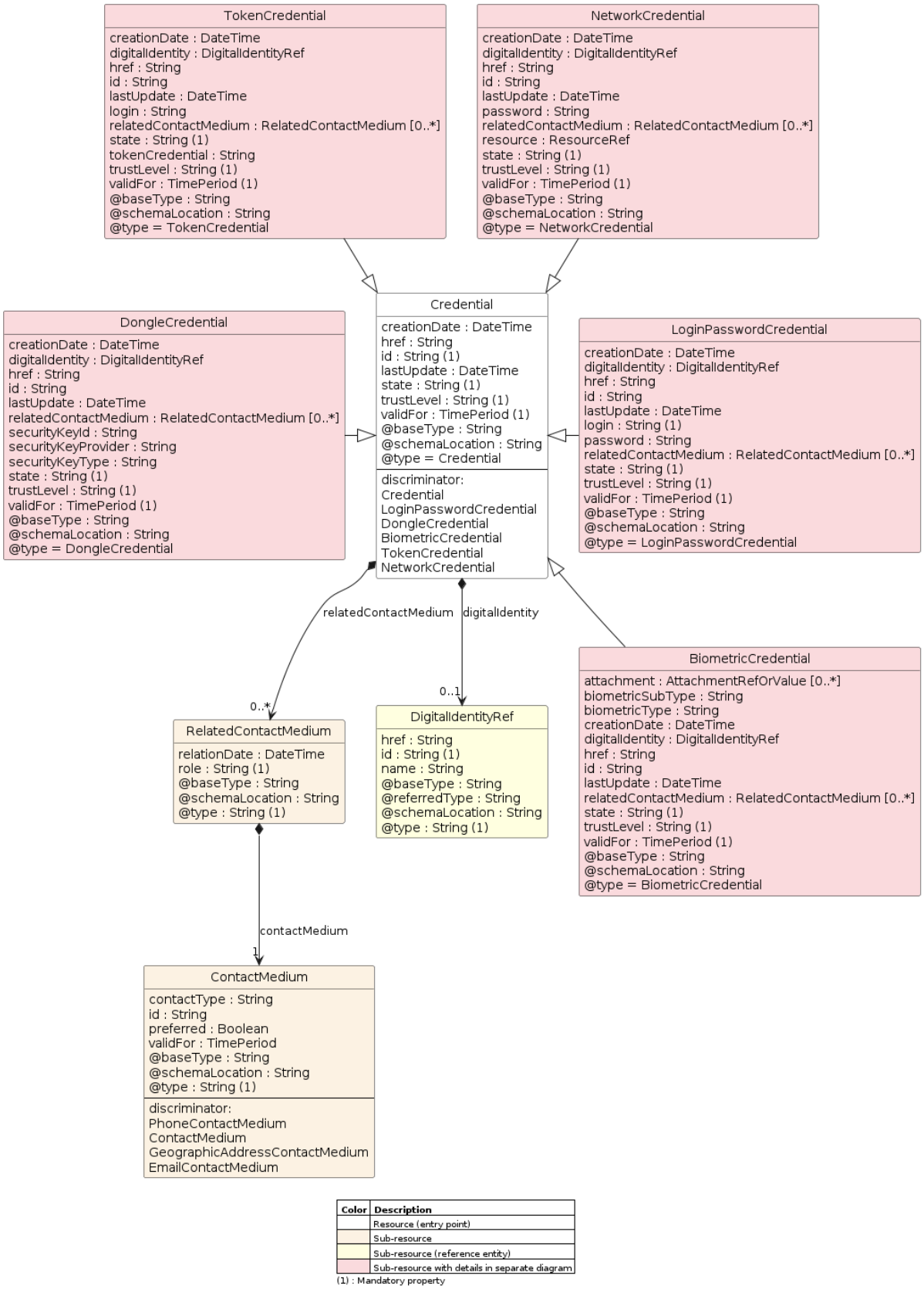


*Figure 9 - Credential*

## Field descriptions

### Credential fields

| | |
|---|---|
| creationDate | A DateTime. Date and time of the Credential creation (timestamp). |
| digitalIdentity | A DigitalIdentityRef. DigitalIdentity reference. |
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| lastUpdate | A DateTime. Date and time of the Credential last update (timestamp). |
| relatedContactMedium | A RelatedContactMedium. A ContactMedium and an associated role such as digital-id-recovery-email, digital-id-recovery-phone, digital-id-2nd-factor-email, digital-id-2nd-factor-phone, credential-login-alias-email, credential-login-alias-phone. |
| state | A String. Active (The credential is currently active and can be used for authentication.), Inactive (The credential is inactive and cannot be used for authentication. This status might occur if the user requested to deactivate the credential temporarily), Expired (The credential has passed its expiration date and cannot be used for authentication. Users may need to renew or update their credential to regain access.), Locked (The credential has been temporarily locked due to multiple failed authentication attempts or security policy violations. This status prevents the credential from being used until it's unlocked by an administrator or through a predefined process.), Revoked (The credential has been permanently revoked, usually due to security concerns or policy violations. Once revoked, the credential cannot be used for authentication and may require additional actions to reinstate.) Pending (The credential is awaiting approval or activation. This status is common for newly created credentials that require administrative review or user verification before becoming active.), Suspended )The credential has been temporarily suspended, often due to a security investigation or compliance issue. While suspended, the credential cannot be used for authentication until the suspension is lifted.), Disabled (Similar to inactive, this status indicates that the credential is currently disabled and cannot be used for authentication. However, unlike inactive, disabled status may imply a more permanent state or administrative action.), Unverified (The credential has been created but not yet verified. Users may need to complete additional steps to verify their identity before the credential becomes active.), Compromised (The credential has been compromised or suspected of being compromised. This status is used to indicate potential security breaches, and immediate action is required to mitigate risks, such as resetting the credential or investigating further.). |
| trustLevel | A String. A level of assurance associated with this credential - this could be used to limit/allow specific permission based on this trust level. |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |

| | |
|---|---|
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |
| | Credential can be instanciated as<br>* BiometricCredential<br>* DongleCredential<br>* LoginPasswordCredential<br>* NetworkCredential<br>* TokenCredential |
| attachment | This property is present in subclasses |
| biometricSubType | This property is present in subclasses |
| biometricType | This property is present in subclasses |
| login | This property is present in subclasses |
| password | This property is present in subclasses |
| resource | This property is present in subclasses |
| securityKeyId | This property is present in subclasses |
| securityKeyProvider | This property is present in subclasses |
| securityKeyType | This property is present in subclasses |
| tokenCredential | This property is present in subclasses |

### RelatedContactMedium sub-resource fields

| | |
|---|---|
| contactMedium | A ContactMedium. Indicates the contact medium that could be used to contact the party. This is an abstract base class, the actual value is in one of the strongly-typed subclasses : EmailContactMedium, FaxContactMedium, PhoneContactMedium, GeographicAddressContactMedium, SocialMediaContactMedium…<br><br>ContactMedium can be instanciated as<br>* EmailContactMedium<br>* GeographicAddressContactMedium<br>* PhoneContactMedium |
| relationDate | A DateTime. Date and time when related contact medium was created. |
| role | A String. Role played by related contact medium. E.g: digital-id-recovery-email, digital-id-recovery-phone, digital-id-2nd-factor-email, digital-id-2nd-factor-phone, credential-login-alias-email, credential-login-alias-phone. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |

| | |
|---|---|
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### DigitalIdentityRef sub-resource fields

| | |
|---|---|
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| name | A String. Name of the referred entity. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @referredType | A String. The actual type of the target instance when needed for disambiguation. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### ContactMedium sub-resource fields

| | |
|---|---|
| contactType | A String. Type of the contact medium to qualify it like pro email / personal email. This is not used to define the contact medium used. |
| id | A String. Identifier for this contact medium. |
| preferred | A Boolean. If true, indicates that is the preferred contact medium. |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |
| | ContactMedium can be instanciated as<br>* EmailContactMedium<br>* GeographicAddressContactMedium<br>* PhoneContactMedium |
| city | This property is present in subclasses |
| country | This property is present in subclasses |
| emailAddress | This property is present in subclasses |
| geographicAddress | This property is present in subclasses |
| phoneNumber | This property is present in subclasses |
| postCode | This property is present in subclasses |
| stateOrProvince | This property is present in subclasses |
| street1 | This property is present in subclasses |

| | |
|---|---|
| street2 | This property is present in subclasses |

### PhoneContactMedium sub-resource fields

| | |
|---|---|
| contactType | A String. Type of the contact medium to qualify it like pro email / personal email. This is not used to define the contact medium used. |
| id | A String. Identifier for this contact medium. |
| phoneNumber | A String. The phone number of the contact. |
| preferred | A Boolean. If true, indicates that is the preferred contact medium. |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### GeographicAddressContactMedium sub-resource fields

| | |
|---|---|
| city | A String. The city. |
| contactType | A String. Type of the contact medium to qualify it like pro email / personal email. This is not used to define the contact medium used. |
| country | A String. The country. |
| geographicAddress | A GeographicAddressRef. Reference to a Geographic Address. |
| id | A String. Identifier for this contact medium. |
| postCode | A String. Postcode. |
| preferred | A Boolean. If true, indicates that is the preferred contact medium. |
| stateOrProvince | A String. State or province. |
| street1 | A String. Describes the street. |
| street2 | A String. Complementary street description. |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### EmailContactMedium sub-resource fields

| | |
|---|---|
| contactType | A String. Type of the contact medium to qualify it like pro email / personal email. This is not used to define the contact medium used. |
| emailAddress | A String. Full email address in standard format. |
| id | A String. Identifier for this contact medium. |
| preferred | A Boolean. If true, indicates that is the preferred contact medium. |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### GeographicAddressRef sub-resource fields

| | |
|---|---|
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| name | A String. Name of the referred entity. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @referredType | A String. The actual type of the target instance when needed for disambiguation. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### Attachment sub-resource fields

| | |
|---|---|
| attachmentType | A String. A business characterization of the purpose of the attachment, for example logo, instructionManual, contractCopy. |
| content | A Base64. The actual contents of the attachment object, if embedded, encoded as base64. |
| description | A String. A narrative text describing the content of the attachment. |
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| mimeType | A String. A technical characterization of the attachment content format using IETF Mime Types. |
| name | A String. The name of the attachment. |
| size | A Quantity. An amount in a given unit. |

| | |
|---|---|
| url | A String. Uniform Resource Locator, is a web page address (a subset of URI). |
| validFor | A TimePeriod. A period of time, either as a deadline (endDateTime only) a startDateTime only, or both. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### AttachmentRef sub-resource fields

| | |
|---|---|
| description | A String. A narrative text describing the content of the attachment. |
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| name | A String. Name of the referred entity. |
| url | A String. Link to the attachment media/content. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @referredType | A String. The actual type of the target instance when needed for disambiguation. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### ResourceRef sub-resource fields

| | |
|---|---|
| href | A String. Hyperlink reference. |
| id | A String. Unique identifier. |
| name | A String. Name of the referred entity. |
| @baseType | A String. When sub-classing, this defines the super-class. |
| @referredType | A String. The actual type of the target instance when needed for disambiguation. |
| @schemaLocation | A String. A URI to a JSON-Schema file that defines additional attributes and relationships. |
| @type | A String. When sub-classing, this defines the sub-class Extensible name. |

### Json representation sample(s)

We provide below a JSON representation as example of the 'Credential' resource object.

```
{
    "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/credential/41af4b86e0b144cb9099b3d4c3ab26ae",
    "id": "41af4b86e0b144cb9099b3d4c3ab26ae",
    "@type": "Credential",
    "state": "Active",
    "validFor": {
       "startDateTime": "2018-09-21T23:20:50.52Z"
    },
    "trustLevel": "high",
    "creationDate": "2018-09-21T09:13:16-07:00",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
 }
```


## Notification Resource Models

10 notifications are defined for this API.

Notifications related to DigitalIdentity:

- Create Event
- Delete Event
- Attribute Value Change Event
- State Change Event

Notifications related to CheckCredential:

- Create Event
- State Change Event

Notifications related to Credential:

- Create Event
- Delete Event
- Attribute Value Change Event
- State Change Event

The notification structure for all notifications in this API follow the pattern depicted by the figure below. A notification event resource (depicted by "SpecificEvent" placeholder) is a sub class of a generic Event structure containing at least an id of the event occurrence (eventId), an event timestamp (eventTime), and the name of the resource (eventType). This notification structure owns an event payload structure ("SpecificEventPayload" placeholder) linked to the resource concerned by the notification using the resource name as access field ("resourceName" placeholder).

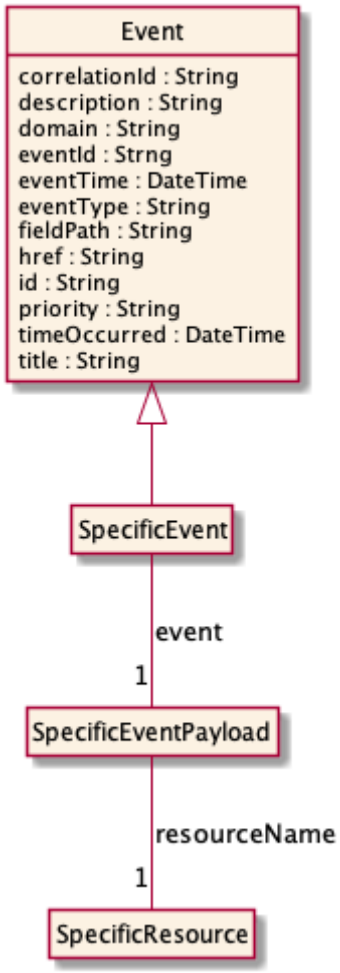


*Figure 10 Notification Pattern*

## DigitalIdentity

### Create Event

Message example for DigitalIdentityCreate Event Notification

```
Content-Type: application/json

{
   "correlationId": "95003dd3-e325",
   "description": "DigitalIdentityCreateEvent illustration",
   "domain": "Commercial",
   "eventId": "4010-9b59-509a64cf85a8",
   "eventTime": "2022-08-25T12:18:12.171Z",
   "eventType": "DigitalIdentityCreateEvent",
   "priority": "1",
   "timeOccurred": "2022-08-25T12:18:06.252Z",
   "title": "DigitalIdentityCreateEvent",
   "event": {
      "digitalIdentity": {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/digitalIdentity/2391ee4acbc142b1a4b74b4d4ab38152",
         "id": "2391ee4acbc142b1a4b74b4d4ab38152",
         "@type": "DigitalIdentity",
```

```
         "nickname": "Neo",
         "state": "Active",
         "validFor": {
            "startDateTime": "2018-09-21T23:20:50.52Z"
         },
         "credential": [
            {
               "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/loginPasswordCredential/41af4b86e0b144cb9099b3d4c3a
b26ae",
               "id": "41af4b86e0b144cb9099b3d4c3ab26ae",
               "@type": "LoginPasswordCredential",
               "@baseType": "Credential",
               "state": "Active",
               "validFor": {
                  "startDateTime": "2018-09-21T23:20:50.52Z"
               },
               "trustLevel": "high",
               "relatedContactMedium": [
                  {
                     "@type": "RelatedContactMedium",
                     "role": "credential-login-alias-email",
                     "contactMedium": {
                        "@type": "EmailContactMedium",
                        "@baseType": "ContactMedium",
                        "contactType": "private",
                        "id": "b2fe04a7f96e479195a47710abcf72be",
                        "preferred": true,
                        "validFor": {
                           "startDateTime": "2018-09-21T23:20:50.52Z"
                        },
                        "emailAddress": "neo@matrix.com"
                     },
                     "relationDate": "2018-09-21T23:20:50.52Z"
                  },
                  {
                     "@type": "RelatedContactMedium",
                     "role": "credential-login-alias-phone",
                     "contactMedium": {
                        "@type": "PhoneContactMedium",
                        "@baseType": "ContactMedium",
                        "contactType": "private",
                        "id": "c0181f3d83e144a59162fd6136a98462",
                        "preferred": true,
                        "validFor": {
                           "startDateTime": "2018-09-21T23:20:50.52Z"
                        },
                        "phoneNumber": "+1 202-918-2132"
                     },
                     "relationDate": "2018-09-21T23:20:50.52Z"
                  }
               ],
               "login": "neo1999",
               "creationDate": "2018-09-21T09:13:16-07:00",
               "lastUpdate": "2018-09-21T23:20:50.52Z"
            }
         ],
         "relatedContactMedium": [
            {
               "@type": "RelatedContactMedium",
               "role": "digital-id-recovery-email",
               "contactMedium": {
                  "@type": "EmailContactMedium",
```

```
                "@baseType": "ContactMedium",
                "contactType": "private",
                "id": "b2fe04a7f96e479195a47710abcf72be",
                "preferred": true,
                "validFor": {
                   "startDateTime": "2018-09-21T23:20:50.52Z"
                },
                "emailAddress": "neo@matrix.com"
             },
             "relationDate": "2018-09-21T23:20:50.52Z"
          },
          {
             "@type": "RelatedContactMedium",
             "role": "digital-id-recovery-phone",
             "contactMedium": {
                "@type": "PhoneContactMedium",
                "@baseType": "ContactMedium",
                "contactType": "private",
                "id": "60703a48038e4fc9a46bf1459aa3590f",
                "preferred": false,
                "validFor": {
                   "startDateTime": "2018-09-21T23:20:50.52Z"
                },
                "phoneNumber": "+1 202-918-2132"
             },
             "relationDate": "2018-09-21T23:20:50.52Z"
          },
          {
             "@type": "RelatedContactMedium",
             "role": "digital-id-2nd-factor-phone",
             "contactMedium": {
                "@type": "PhoneContactMedium",
                "@baseType": "ContactMedium",
                "contactType": "private",
                "id": "c0181f3d83e144a59162fd6136a98462",
                "preferred": true,
                "validFor": {
                   "startDateTime": "2018-09-21T23:20:50.52Z"
                },
                "phoneNumber": "+1 202-918-2132"
             },
             "relationDate": "2018-09-21T23:20:50.52Z"
          }
       ],
       "attachment": [
          {
             "@type": "Attachment",
             "attachmentType": "avatarPicture",
             "name": "Neo's avatar",
             "url": "https://i.pravatar.cc/150?u=neo",
             "mimeType": "image/jpeg",
             "size": {
                "amount": 91,
                "units": "Kb"
             },
             "validFor": {
                "startDateTime": "2018-09-21T23:20:50.52Z"
             }
          }
       ],
       "partyRoleIdentified": [
          {
             "@type": "RelatedSecurityPrincipalRef",
```

```
                "role": "Customer",
                "securityPrincipalRef": {
                   "href": "https://serverRoot/tmf-
api/customerManagement/v5/partyRole/faa43dccaad142289e2b0f0e73e15958",
                   "id": "faa43dccaad142289e2b0f0e73e15958",
                   "@type": "PartyRoleRef",
                   "@referredType": "PartyRole"
                }
             }
          ],
          "individualIdentified": {
             "href": "https://serverRoot/tmf-
api/partyManagement/v5/individual/193c8d6887394ca5b50290685db512ca",
             "id": "193c8d6887394ca5b50290685db512ca",
             "@type": "IndividualRef",
             "@referredType": "Individual"
          },
          "relatedSecurityPrincipal": [
             {
                "@type": "RelatedSecurityPrincipalRef",
                "role": "ServiceProvider",
                "securityPrincipalRef": {
                   "href": "https://serverRoot/tmf-
api/partyManagement/v5/organization/e9b93f395a11453f9b7aa3349e857c24",
                   "id": "e9b93f395a11453f9b7aa3349e857c24",
                   "@type": "OrganizationRef",
                   "@referredType": "Organization",
                   "name": "Acme Inc."
                }
             },
             {
                "@type": "RelatedSecurityPrincipalRef",
                "role": "DigitalIdentityProvider",
                "securityPrincipalRef": {
                   "href": "https://serverRoot/tmf-
api/partyManagement/v5/organization/af08cfda572749b0b4a90dfb75dfca51",
                   "id": "af08cfda572749b0b4a90dfb75dfca51",
                   "@type": "OrganizationRef",
                   "@referredType": "Organization",
                   "name": "Auth0"
                }
             }
          ],
          "creationDate": "2018-09-21T09:13:16-07:00",
          "lastUpdate": "2018-09-21T23:20:50.52Z"
       }
    },
    "reportingSystem": {
       "id": "759",
       "name": "APP-745",
       "@type": "ReportingResource",
       "@referredType": "LogicalResource"
    },
    "source": {
       "id": "705",
       "name": "APP-317",
       "@type": "ReportingResource",
       "@referredType": "LogicalResource"
    },
    "@baseType": "Event",
    "@type": "DigitalIdentityCreateEvent"
}
```

### Delete Event

Message example for DigitalIdentityDelete Event Notification

```
Content-Type: application/json

{
   "correlationId": "90cfc73d-deb7",
   "description": "DigitalIdentityDeleteEvent illustration",
   "domain": "Commercial",
   "eventId": "47d6-9751-40e4f01440c9",
   "eventTime": "2022-08-25T12:18:12.202Z",
   "eventType": "DigitalIdentityDeleteEvent",
   "priority": "4",
   "timeOccurred": "2022-08-25T12:18:07.224Z",
   "title": "DigitalIdentityDeleteEvent",
   "event": {
      "digitalIdentity": {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/digitalIdentity/2391ee4acbc142b1a4b74b4d4ab38152",
         "id": "2391ee4acbc142b1a4b74b4d4ab38152",
         "@type": "DigitalIdentity"
      }
   },
   "reportingSystem": {
      "id": "759",
      "name": "APP-745",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "source": {
      "id": "705",
      "name": "APP-317",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "@baseType": "Event",
   "@type": "DigitalIdentityDeleteEvent"
}
```

### Attribute Value Change Event

Message example for DigitalIdentityAttributeValueChange Event Notification

```
Content-Type: application/json

{
   "correlationId": "333-fd6",
   "description": "DigitalIdentityAttributeValueChangeEvent illustration",
   "domain": "Commercial",
   "eventId": "569",
   "eventTime": "2021-09-27T07:43:59.059Z",
   "eventType": "DigitalIdentityAttributeValueChangeEvent",
   "priority": "1",
   "timeOccurred": "2021-09-27T07:43:59.059Z",
   "title": "DigitalIdentityAttributeValueChangeEvent",
   "event": {
      "digitalIdentity": {
```

```
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/digitalIdentity/2391ee4acbc142b1a4b74b4d4ab38152",
         "id": "2391ee4acbc142b1a4b74b4d4ab38152",
         "@type": "DigitalIdentity",
         "nickname": "Neo",
         "validFor": {
            "startDateTime": "2018-09-21T23:20:50.52Z"
         }
      }
   },
   "reportingSystem": {
      "id": "123",
      "name": "CRM app",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "source": {
      "id": "123",
      "name": "CRM app",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "@baseType": "Event",
   "@type": "DigitalIdentityAttributeValueChangeEvent"
}
```


### State Change Event

Message example for DigitalIdentityStateChange Event Notification


```
Content-Type: application/json

{
   "correlationId": "0f874cb9-c70d",
   "description": "DigitalIdentityStateChangeEvent illustration",
   "domain": "Commercial",
   "eventId": "41cf-ad81-d65ea1c2840c",
   "eventTime": "2022-08-25T12:18:12.191Z",
   "eventType": "DigitalIdentityStateChangeEvent",
   "priority": "5",
   "timeOccurred": "2022-08-25T12:18:08.202Z",
   "title": "DigitalIdentityStateChangeEvent",
   "event": {
      "digitalIdentity": {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/digitalIdentity/2391ee4acbc142b1a4b74b4d4ab38152",
         "id": "2391ee4acbc142b1a4b74b4d4ab38152",
         "@type": "DigitalIdentity",
         "state": "Active"
      }
   },
   "reportingSystem": {
      "id": "759",
      "name": "APP-745",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "source": {
      "id": "705",
      "name": "APP-317",
```

```
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "@baseType": "Event",
   "@type": "DigitalIdentityStateChangeEvent"
}
```

## CheckCredential

### Create Event

Message example for CheckCredentialCreateEvent Event Notification

```
Content-Type: application/json

{
   "correlationId": "95003dd3-e325",
   "description": "CheckCredentialCreateEvent illustration",
   "domain": "Commercial",
   "eventId": "4010-9b59-509a64cf85a8",
   "eventTime": "2022-08-25T12:18:12.171Z",
   "eventType": "CheckCredentialCreateEvent",
   "priority": "1",
   "timeOccurred": "2022-08-25T12:18:06.252Z",
   "title": "CheckCredentialCreateEvent",
   "event": {
      "checkCredential": {
         "id": "bf0fc07cff1946079548b7edb0d0db05",
         "@type": "CheckCredential",
         "credential": {
            "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/loginPasswordCredential/41af4b86e0b144cb9099b3d4c3a
b26ae",
            "id": "41af4b86e0b144cb9099b3d4c3ab26ae",
            "@type": "LoginPasswordCredential",
            "@baseType": "Credential",
            "state": "Active",
            "validFor": {
               "startDateTime": "2018-09-21T23:20:50.52Z"
            },
            "trustLevel": "high",
            "login": "neo1999",
            "digitalIdentity": {
               "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/digitalIdentity/2391ee4acbc142b1a4b74b4d4ab38152",
               "id": "2391ee4acbc142b1a4b74b4d4ab38152",
               "@type": "DigitalIdentityRef",
               "@referredType": "DigitalIdentity"
            },
            "creationDate": "2018-09-21T09:13:16-07:00",
            "lastUpdate": "2018-09-21T23:20:50.52Z"
         },
         "creationDate": "2018-09-21T09:13:16-07:00",
         "status": "succeded",
         "lastUpdate": "2018-09-21T23:20:50.52Z"
      }
   },
   "reportingSystem": {
      "id": "759",
```

```
      "name": "APP-745",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "source": {
      "id": "705",
      "name": "APP-317",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "@baseType": "Event",
   "@type": "CheckCredentialCreateEvent"
}
```


### State Change Event

Message example for CheckCredentialStateChangeEvent Event Notification


```
Content-Type: application/json

{
   "correlationId": "0f874cb9-c70d",
   "description": "CheckCredentialStateChangeEvent illustration",
   "domain": "Commercial",
   "eventId": "41cf-ad81-d65ea1c2840c",
   "eventTime": "2022-08-25T12:18:12.191Z",
   "eventType": "CheckCredentialStateChangeEvent",
   "priority": "5",
   "timeOccurred": "2022-08-25T12:18:08.202Z",
   "title": "CheckCredentialStateChangeEvent",
   "event": {
      "checkCredential": {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/checkCredential/bf0fc07cff1946079548b7edb0d0db05",
         "id": "bf0fc07cff1946079548b7edb0d0db05",
         "@type": "CheckCredential",
         "status": "succeded",
         "lastUpdate": "2018-09-21T23:20:50.52Z"
      }
   },
   "reportingSystem": {
      "id": "759",
      "name": "APP-745",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "source": {
      "id": "705",
      "name": "APP-317",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "@baseType": "Event",
   "@type": "CheckCredentialStateChangeEvent"
}
```

## Credential

### Create Event

### Sample: Biometric Credential Create Notification example

Message example for Biometric Credential Create Event Notification

```
Content-Type: application/json

{
   "correlationId": "95003dd3-e325",
   "description": "BiometricCredentialCreateEvent illustration",
   "domain": "Commercial",
   "eventId": "4010-9b59-509a64cf85a8",
   "eventTime": "2022-08-25T12:18:12.171Z",
   "eventType": "CredentialCreateEvent",
   "priority": "1",
   "timeOccurred": "2022-08-25T12:18:06.252Z",
   "title": "BiometricCredentialCreateEvent",
   "event": {
      "credential": {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/biometricCredential/754ea8ed4bef49d78ca2ba3f953cd65
f",
         "id": "754ea8ed4bef49d78ca2ba3f953cd65f",
         "@type": "BiometricCredential",
         "@baseType": "Credential",
         "state": "Active",
         "validFor": {
            "startDateTime": "2018-09-21T23:20:50.52Z"
         },
         "trustLevel": "high",
         "biometricType": "finger",
         "biometricSubType": "thumb",
         "attachment": [
            {
               "@type": "Attachment",
               "attachmentType": "thumbFingerprint",
               "name": "Thumb fingerprint",
               "content": "d2VyZndlcmZyd2VyZXJ3Zn...",
               "mimeType": "image/png",
               "size": {
                  "amount": 104,
                  "units": "Kb"
               },
               "validFor": {
                  "startDateTime": "2018-09-21T23:20:50.52Z"
               }
            }
         ],
         "creationDate": "2018-09-21T09:13:16-07:00",
         "lastUpdate": "2018-09-21T23:20:50.52Z"
      }
   },
   "reportingSystem": {
      "id": "759",
      "name": "APP-745",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
```

```
    },
    "source": {
       "id": "705",
       "name": "APP-317",
       "@type": "ReportingResource",
       "@referredType": "LogicalResource"
    },
    "@baseType": "Event",
    "@type": "CredentialCreateEvent"
}
```


### Sample: Dongle Credential Create Notification example

Message example for Dongle Credential Create Event Notification


```
Content-Type: application/json

{
   "correlationId": "95003dd3-e325",
   "description": "DongleCredentialCreateEvent illustration",
   "domain": "Commercial",
   "eventId": "4010-9b59-509a64cf85a8",
   "eventTime": "2022-08-25T12:18:12.171Z",
   "eventType": "CredentialCreateEvent",
   "priority": "1",
   "timeOccurred": "2022-08-25T12:18:06.252Z",
   "title": "DongleCredentialCreateEvent",
   "event": {
      "credential": {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/dongleCredential/f4435d1e425a420da6e80abb4c075b22",
         "id": "f4435d1e425a420da6e80abb4c075b22",
         "@type": "DongleCredential",
         "@baseType": "Credential",
         "state": "Active",
         "validFor": {
            "startDateTime": "2018-09-21T23:20:50.52Z"
         },
         "trustLevel": "high",
         "securityKeyId": "AE7671DF35BD581F467AB9B3DCF92",
         "securityKeyType": "USB Security Key",
         "securityKeyProvider": "Yubico",
         "creationDate": "2018-09-21T09:13:16-07:00",
         "lastUpdate": "2018-09-21T23:20:50.52Z"
      }
   },
   "reportingSystem": {
      "id": "759",
      "name": "APP-745",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "source": {
      "id": "705",
      "name": "APP-317",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "@baseType": "Event",
   "@type": "CredentialCreateEvent"
```

```
}
```

### Sample: Login Password Credential Create Notification example

Message example for Login Password Credential Create Event Notification

```
Content-Type: application/json

{
   "correlationId": "95003dd3-e325",
   "description": "LoginPasswordCredentialCreateEvent illustration",
   "domain": "Commercial",
   "eventId": "4010-9b59-509a64cf85a8",
   "eventTime": "2022-08-25T12:18:12.171Z",
   "eventType": "CredentialCreateEvent",
   "priority": "1",
   "timeOccurred": "2022-08-25T12:18:06.252Z",
   "title": "LoginPasswordCredentialCreateEvent",
   "event": {
      "credential": {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/loginPasswordCredential/41af4b86e0b144cb9099b3d4c3a
b26ae",
         "id": "41af4b86e0b144cb9099b3d4c3ab26ae",
         "@type": "LoginPasswordCredential",
         "@baseType": "Credential",
         "state": "Active",
         "validFor": {
            "startDateTime": "2018-09-21T23:20:50.52Z"
         },
         "trustLevel": "high",
         "relatedContactMedium": [
            {
               "@type": "RelatedContactMedium",
               "role": "credential-login-alias-email",
               "contactMedium": {
                  "@type": "EmailContactMedium",
                  "@baseType": "ContactMedium",
                  "contactType": "private",
                  "id": "b2fe04a7f96e479195a47710abcf72be",
                  "preferred": true,
                  "validFor": {
                     "startDateTime": "2018-09-21T23:20:50.52Z"
                  },
                  "emailAddress": "neo@matrix.com"
               },
               "relationDate": "2018-09-21T23:20:50.52Z"
            },
            {
               "@type": "RelatedContactMedium",
               "role": "credential-login-alias-phone",
               "contactMedium": {
                  "@type": "PhoneContactMedium",
                  "@baseType": "ContactMedium",
                  "contactType": "private",
                  "id": "c0181f3d83e144a59162fd6136a98462",
                  "preferred": true,
                  "validFor": {
                     "startDateTime": "2018-09-21T23:20:50.52Z"
                  },
```

```
                  "phoneNumber": "+1 202-918-2132"
               },
               "relationDate": "2018-09-21T23:20:50.52Z"
            }
         ],
         "login": "neo1999",
         "creationDate": "2018-09-21T09:13:16-07:00",
         "lastUpdate": "2018-09-21T23:20:50.52Z"
      }
   },
   "reportingSystem": {
      "id": "759",
      "name": "APP-745",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "source": {
      "id": "705",
      "name": "APP-317",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "@baseType": "Event",
   "@type": "CredentialCreateEvent"
}
```


### Sample: Network Credential Create Notification example

Message example for Network Credential Create Event Notification


```
Content-Type: application/json

{
   "correlationId": "95003dd3-e325",
   "description": "NetworkCredentialCreateEvent illustration",
   "domain": "Commercial",
   "eventId": "4010-9b59-509a64cf85a8",
   "eventTime": "2022-08-25T12:18:12.171Z",
   "eventType": "CredentialCreateEvent",
   "priority": "1",
   "timeOccurred": "2022-08-25T12:18:06.252Z",
   "title": "NetworkCredentialCreateEvent",
   "event": {
      "credential": {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/networkCredential/9fd97c82b4bf4fe7bcbee314d811290b"
,
         "id": "9fd97c82b4bf4fe7bcbee314d811290b",
         "@type": "NetworkCredential",
         "@baseType": "Credential",
         "state": "Active",
         "validFor": {
            "startDateTime": "2018-09-21T23:20:50.52Z"
         },
         "trustLevel": "high",
         "resource": {
            "@type": "ResourceRef",
            "id": "99729be76fa948d5a1df22618bec96ea"
         },
         "creationDate": "2018-09-21T09:13:16-07:00",
```

```
            "lastUpdate": "2018-09-21T23:20:50.52Z"
         }
      },
      "reportingSystem": {
         "id": "759",
         "name": "APP-745",
         "@type": "ReportingResource",
         "@referredType": "LogicalResource"
      },
      "source": {
         "id": "705",
         "name": "APP-317",
         "@type": "ReportingResource",
         "@referredType": "LogicalResource"
      },
      "@baseType": "Event",
      "@type": "CredentialCreateEvent"
   }
```


### Sample: Token Credential Create Notification example

Message example for Token Credential Create Event Notification


```
Content-Type: application/json

{
   "correlationId": "95003dd3-e325",
   "description": "TokenCredentialCreateEvent illustration",
   "domain": "Commercial",
   "eventId": "4010-9b59-509a64cf85a8",
   "eventTime": "2022-08-25T12:18:12.171Z",
   "eventType": "CredentialCreateEvent",
   "priority": "1",
   "timeOccurred": "2022-08-25T12:18:06.252Z",
   "title": "TokenCredentialCreateEvent",
   "event": {
      "credential": {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/tokenCredential/7ef64b30fd5345ac9ab9554798c21f5c",
         "id": "7ef64b30fd5345ac9ab9554798c21f5c",
         "@type": "TokenCredential",
         "@baseType": "Credential",
         "state": "Active",
         "validFor": {
            "startDateTime": "2018-09-21T23:20:50.52Z",
            "endDateTime": "2018-10-21T23:20:50.52Z"
         },
         "trustLevel": "high",
         "login": "google.id:107691503500061507151130823 67",
         "tokenCredential":
"6nxugrzcv0e4se81kufqf0nn0rpygf4yqzyp7gha68wgqdpm057lx97jiiy6fdpq",
         "creationDate": "2018-09-21T09:13:16-07:00",
         "lastUpdate": "2018-09-21T23:20:50.52Z"
      }
   },
   "reportingSystem": {
      "id": "759",
      "name": "APP-745",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
```

```
    },
    "source": {
       "id": "705",
       "name": "APP-317",
       "@type": "ReportingResource",
       "@referredType": "LogicalResource"
    },
    "@baseType": "Event",
    "@type": "CredentialCreateEvent"
}
```


### Delete Event

### Sample: Biometric Credential Delete Notification example

Message example for Biometric Credential Delete Event Notification


```
Content-Type: application/json

{
   "correlationId": "90cfc73d-deb7",
   "description": "BiometricCredentialDeleteEvent illustration",
   "domain": "Commercial",
   "eventId": "47d6-9751-40e4f01440c9",
   "eventTime": "2022-08-25T12:18:12.202Z",
   "eventType": "CredentialDeleteEvent",
   "priority": "4",
   "timeOccurred": "2022-08-25T12:18:07.224Z",
   "title": "BiometricCredentialDeleteEvent",
   "event": {
      "credential": {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/biometricCredential/754ea8ed4bef49d78ca2ba3f953cd65
f",
         "id": "754ea8ed4bef49d78ca2ba3f953cd65f",
         "@type": "BiometricCredential"
      }
   },
   "reportingSystem": {
      "id": "759",
      "name": "APP-745",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "source": {
      "id": "705",
      "name": "APP-317",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "@baseType": "Event",
   "@type": "CredentialDeleteEvent"
}
```


### Sample: Dongle Credential Delete Notification example

Message example for Dongle Credential Delete Event Notification

```
Content-Type: application/json

{
   "correlationId": "90cfc73d-deb7",
   "description": "DongleCredentialDeleteEvent illustration",
   "domain": "Commercial",
   "eventId": "47d6-9751-40e4f01440c9",
   "eventTime": "2022-08-25T12:18:12.202Z",
   "eventType": "CredentialDeleteEvent",
   "priority": "4",
   "timeOccurred": "2022-08-25T12:18:07.224Z",
   "title": "DongleCredentialDeleteEvent",
   "event": {
      "credential": {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/dongleCredential/f4435d1e425a420da6e80abb4c075b22",
         "id": "f4435d1e425a420da6e80abb4c075b22",
         "@type": "DongleCredential"
      }
   },
   "reportingSystem": {
      "id": "759",
      "name": "APP-745",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "source": {
      "id": "705",
      "name": "APP-317",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "@baseType": "Event",
   "@type": "CredentialDeleteEvent"
}
```

### Sample: Login Password Credential Delete Notification example

Message example for Login Password Credential Delete Event Notification

```
Content-Type: application/json

{
   "correlationId": "90cfc73d-deb7",
   "description": "LoginPasswordCredentialDeleteEvent illustration",
   "domain": "Commercial",
   "eventId": "47d6-9751-40e4f01440c9",
   "eventTime": "2022-08-25T12:18:12.202Z",
   "eventType": "CredentialDeleteEvent",
   "priority": "4",
   "timeOccurred": "2022-08-25T12:18:07.224Z",
   "title": "LoginPasswordCredentialDeleteEvent",
   "event": {
      "credential": {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/loginPasswordCredential/41af4b86e0b144cb9099b3d4c3a
b26ae",
         "id": "41af4b86e0b144cb9099b3d4c3ab26ae",
         "@type": "LoginPasswordCredential"
```

```
      }
   },
   "reportingSystem": {
      "id": "759",
      "name": "APP-745",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "source": {
      "id": "705",
      "name": "APP-317",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "@baseType": "Event",
   "@type": "CredentialDeleteEvent"
}
```

**Sample: Network Credential Delete Notification example**

Message example for Network Credential Delete Event Notification

```
Content-Type: application/json

{
   "correlationId": "90cfc73d-deb7",
   "description": "NetworkCredentialDeleteEvent illustration",
   "domain": "Commercial",
   "eventId": "47d6-9751-40e4f01440c9",
   "eventTime": "2022-08-25T12:18:12.202Z",
   "eventType": "CredentialDeleteEvent",
   "priority": "4",
   "timeOccurred": "2022-08-25T12:18:07.224Z",
   "title": "NetworkCredentialDeleteEvent",
   "event": {
      "credential": {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/networkCredential/9fd97c82b4bf4fe7bcbee314d811290b"
,
         "id": "9fd97c82b4bf4fe7bcbee314d811290b",
         "@type": "NetworkCredential"
      }
   },
   "reportingSystem": {
      "id": "759",
      "name": "APP-745",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "source": {
      "id": "705",
      "name": "APP-317",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "@baseType": "Event",
   "@type": "CredentialDeleteEvent"
}
```

### Sample: Token Credential Delete Notification example

Message example for Token Credential Delete Event Notification

```
Content-Type: application/json

{
   "correlationId": "90cfc73d-deb7",
   "description": "TokenCredentialDeleteEvent illustration",
   "domain": "Commercial",
   "eventId": "47d6-9751-40e4f01440c9",
   "eventTime": "2022-08-25T12:18:12.202Z",
   "eventType": "CredentialDeleteEvent",
   "priority": "4",
   "timeOccurred": "2022-08-25T12:18:07.224Z",
   "title": "TokenCredentialDeleteEvent",
   "event": {
      "credential": {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/tokenCredential/7ef64b30fd5345ac9ab9554798c21f5c",
         "id": "7ef64b30fd5345ac9ab9554798c21f5c",
         "@type": "TokenCredential"
      }
   },
   "reportingSystem": {
      "id": "759",
      "name": "APP-745",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "source": {
      "id": "705",
      "name": "APP-317",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "@baseType": "Event",
   "@type": "CredentialDeleteEvent"
}
```

### Attribute Value Change Event

### Sample: Biometric Credential Attribute Value Change Notification example

Message example for Biometric Credential Attribute Value Change Event Notification

```
Content-Type: application/json

{
   "correlationId": "333-fd6",
   "description": "BiometricCredentialAttributeValueChangeEvent illustration",
   "domain": "Commercial",
   "eventId": "569",
   "eventTime": "2021-09-27T07:43:59.059Z",
   "eventType": "CredentialAttributeValueChangeEvent",
   "priority": "1",
   "timeOccurred": "2021-09-27T07:43:59.059Z",
   "title": "BiometricCredentialAttributeValueChangeEvent",
```

```
   "event": {
      "credential": {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/biometricCredential/754ea8ed4bef49d78ca2ba3f953cd65
f",
         "id": "754ea8ed4bef49d78ca2ba3f953cd65f",
         "@type": "BiometricCredential",
         "validFor": {
            "startDateTime": "2018-09-21T23:20:50.52Z"
         },
         "trustLevel": "high"
      }
   },
   "reportingSystem": {
      "id": "123",
      "name": "CRM app",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "source": {
      "id": "123",
      "name": "CRM app",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "@baseType": "Event",
   "@type": "CredentialAttributeValueChangeEvent"
}
```


**Sample: Dongle Credential Attribute Value Change Notification example**

Message example for Dongle Credential Attribute Value Change Event Notification


```
Content-Type: application/json

{
   "correlationId": "333-fd6",
   "description": "DongleCredentialAttributeValueChangeEvent illustration",
   "domain": "Commercial",
   "eventId": "569",
   "eventTime": "2021-09-27T07:43:59.059Z",
   "eventType": "CredentialAttributeValueChangeEvent",
   "priority": "1",
   "timeOccurred": "2021-09-27T07:43:59.059Z",
   "title": "DongleCredentialAttributeValueChangeEvent",
   "event": {
      "credential": {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/dongleCredential/f4435d1e425a420da6e80abb4c075b22",
         "id": "f4435d1e425a420da6e80abb4c075b22",
         "@type": "DongleCredential",
         "validFor": {
            "startDateTime": "2018-09-21T23:20:50.52Z"
         },
         "trustLevel": "high"
      }
   },
   "reportingSystem": {
      "id": "123",
      "name": "CRM app",
```

```
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "source": {
      "id": "123",
      "name": "CRM app",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "@baseType": "Event",
   "@type": "CredentialAttributeValueChangeEvent"
}
```


**Sample: Login Password Credential Attribute Value Change Notification example**

Message example for Login Password Credential Attribute Value Change Event Notification


```
Content-Type: application/json

{
   "correlationId": "333-fd6",
   "description": "LoginPasswordCredentialAttributeValueChangeEvent illustration",
   "domain": "Commercial",
   "eventId": "569",
   "eventTime": "2021-09-27T07:43:59.059Z",
   "eventType": "CredentialAttributeValueChangeEvent",
   "priority": "1",
   "timeOccurred": "2021-09-27T07:43:59.059Z",
   "title": "LoginPasswordCredentialAttributeValueChangeEvent",
   "event": {
      "credential": {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/loginPasswordCredential/41af4b86e0b144cb9099b3d4c3a
b26ae",
         "id": "41af4b86e0b144cb9099b3d4c3ab26ae",
         "@type": "LoginPasswordCredential",
         "validFor": {
            "startDateTime": "2018-09-21T23:20:50.52Z"
         },
         "trustLevel": "high"
      }
   },
   "reportingSystem": {
      "id": "123",
      "name": "CRM app",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "source": {
      "id": "123",
      "name": "CRM app",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "@baseType": "Event",
   "@type": "CredentialAttributeValueChangeEvent"
}
```


**Sample: Network Credential Attribute Value Change Notification example**

Message example for Network Credential Attribute Value Change Event Notification


```
Content-Type: application/json

{
   "correlationId": "333-fd6",
   "description": "NetworkCredentialAttributeValueChangeEvent illustration",
   "domain": "Commercial",
   "eventId": "569",
   "eventTime": "2021-09-27T07:43:59.059Z",
   "eventType": "CredentialAttributeValueChangeEvent",
   "priority": "1",
   "timeOccurred": "2021-09-27T07:43:59.059Z",
   "title": "NetworkCredentialAttributeValueChangeEvent",
   "event": {
      "credential": {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/networkCredential/9fd97c82b4bf4fe7bcbee314d811290b"
,
         "id": "9fd97c82b4bf4fe7bcbee314d811290b",
         "@type": "NetworkCredential",
         "validFor": {
            "startDateTime": "2018-09-21T23:20:50.52Z"
         },
         "trustLevel": "high"
      }
   },
   "reportingSystem": {
      "id": "123",
      "name": "CRM app",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "source": {
      "id": "123",
      "name": "CRM app",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "@baseType": "Event",
   "@type": "CredentialAttributeValueChangeEvent"
}
```


**Sample: Token Credential Attribute Value Change Notification example**

Message example for Token Credential Attribute Value Change Event Notification


```
Content-Type: application/json

{
   "correlationId": "333-fd6",
   "description": "TokenCredentialAttributeValueChangeEvent illustration",
   "domain": "Commercial",
   "eventId": "569",
   "eventTime": "2021-09-27T07:43:59.059Z",
   "eventType": "CredentialAttributeValueChangeEvent",
   "priority": "1",
   "timeOccurred": "2021-09-27T07:43:59.059Z",
   "title": "TokenCredentialAttributeValueChangeEvent",
```

```
    "event": {
       "credential": {
          "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/tokenCredential/7ef64b30fd5345ac9ab9554798c21f5c",
          "id": "7ef64b30fd5345ac9ab9554798c21f5c",
          "@type": "TokenCredential",
          "validFor": {
             "startDateTime": "2018-09-21T23:20:50.52Z",
             "endDateTime": "2018-10-21T23:20:50.52Z"
          },
          "trustLevel": "high"
       }
    },
    "reportingSystem": {
       "id": "123",
       "name": "CRM app",
       "@type": "ReportingResource",
       "@referredType": "LogicalResource"
    },
    "source": {
       "id": "123",
       "name": "CRM app",
       "@type": "ReportingResource",
       "@referredType": "LogicalResource"
    },
    "@baseType": "Event",
    "@type": "CredentialAttributeValueChangeEvent"
}
```


### State Change Event

### Sample: Biometric Credential State Change Notification example

Message example for Biometric Credential State Change Event Notification


```
Content-Type: application/json

{
   "correlationId": "0f874cb9-c70d",
   "description": "BiometricCredentialStateChangeEvent illustration",
   "domain": "Commercial",
   "eventId": "41cf-ad81-d65ea1c2840c",
   "eventTime": "2022-08-25T12:18:12.191Z",
   "eventType": "CredentialStateChangeEvent",
   "priority": "5",
   "timeOccurred": "2022-08-25T12:18:08.202Z",
   "title": "BiometricCredentialStateChangeEvent",
   "event": {
      "credential": {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/biometricCredential/754ea8ed4bef49d78ca2ba3f953cd65
f",
         "id": "754ea8ed4bef49d78ca2ba3f953cd65f",
         "@type": "BiometricCredential",
         "state": "Active"
      }
   },
   "reportingSystem": {
      "id": "759",
```

```
      "name": "APP-745",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "source": {
      "id": "705",
      "name": "APP-317",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "@baseType": "Event",
   "@type": "CredentialStateChangeEvent"
}
```


**Sample: Dongle Credential State Change Notification example**

Message example for Dongle Credential State Change Event Notification


```
Content-Type: application/json

{
   "correlationId": "0f874cb9-c70d",
   "description": "DongleCredentialStateChangeEvent illustration",
   "domain": "Commercial",
   "eventId": "41cf-ad81-d65ea1c2840c",
   "eventTime": "2022-08-25T12:18:12.191Z",
   "eventType": "CredentialStateChangeEvent",
   "priority": "5",
   "timeOccurred": "2022-08-25T12:18:08.202Z",
   "title": "DongleCredentialStateChangeEvent",
   "event": {
      "credential": {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/dongleCredential/f4435d1e425a420da6e80abb4c075b22",
         "id": "f4435d1e425a420da6e80abb4c075b22",
         "@type": "DongleCredential",
         "state": "Active"
      }
   },
   "reportingSystem": {
      "id": "759",
      "name": "APP-745",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "source": {
      "id": "705",
      "name": "APP-317",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "@baseType": "Event",
   "@type": "CredentialStateChangeEvent"
}
```


**Sample: Login Password Credential State Change Notification example**

Message example for Login Password Credential State Change Event Notification

```
Content-Type: application/json

{
   "correlationId": "0f874cb9-c70d",
   "description": "LoginPasswordCredentialStateChangeEvent illustration",
   "domain": "Commercial",
   "eventId": "41cf-ad81-d65ea1c2840c",
   "eventTime": "2022-08-25T12:18:12.191Z",
   "eventType": "CredentialStateChangeEvent",
   "priority": "5",
   "timeOccurred": "2022-08-25T12:18:08.202Z",
   "title": "LoginPasswordCredentialStateChangeEvent",
   "event": {
      "credential": {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/loginPasswordCredential/41af4b86e0b144cb9099b3d4c3a
b26ae",
         "id": "41af4b86e0b144cb9099b3d4c3ab26ae",
         "@type": "LoginPasswordCredential",
         "state": "Active"
      }
   },
   "reportingSystem": {
      "id": "759",
      "name": "APP-745",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "source": {
      "id": "705",
      "name": "APP-317",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "@baseType": "Event",
   "@type": "CredentialStateChangeEvent"
}
```

### Sample: Network Credential State Change Notification example

Message example for Network Credential State Change Event Notification

```
Content-Type: application/json

{
   "correlationId": "0f874cb9-c70d",
   "description": "NetworkCredentialStateChangeEvent illustration",
   "domain": "Commercial",
   "eventId": "41cf-ad81-d65ea1c2840c",
   "eventTime": "2022-08-25T12:18:12.191Z",
   "eventType": "CredentialStateChangeEvent",
   "priority": "5",
   "timeOccurred": "2022-08-25T12:18:08.202Z",
   "title": "NetworkCredentialStateChangeEvent",
   "event": {
      "credential": {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/networkCredential/9fd97c82b4bf4fe7bcbee314d811290b"
,
```

```
            "id": "9fd97c82b4bf4fe7bcbee314d811290b",
            "@type": "NetworkCredential",
            "state": "Active"
         }
      },
      "reportingSystem": {
         "id": "759",
         "name": "APP-745",
         "@type": "ReportingResource",
         "@referredType": "LogicalResource"
      },
      "source": {
         "id": "705",
         "name": "APP-317",
         "@type": "ReportingResource",
         "@referredType": "LogicalResource"
      },
      "@baseType": "Event",
      "@type": "CredentialStateChangeEvent"
   }
```


### Sample: Token Credential State Change Notification example

Message example for Token Credential State Change Event Notification


```
Content-Type: application/json

{
   "correlationId": "0f874cb9-c70d",
   "description": "TokenCredentialStateChangeEvent illustration",
   "domain": "Commercial",
   "eventId": "41cf-ad81-d65ea1c2840c",
   "eventTime": "2022-08-25T12:18:12.191Z",
   "eventType": "CredentialStateChangeEvent",
   "priority": "5",
   "timeOccurred": "2022-08-25T12:18:08.202Z",
   "title": "TokenCredentialStateChangeEvent",
   "event": {
      "credential": {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/tokenCredential/7ef64b30fd5345ac9ab9554798c21f5c",
         "id": "7ef64b30fd5345ac9ab9554798c21f5c",
         "@type": "TokenCredential",
         "state": "Active"
      }
   },
   "reportingSystem": {
      "id": "759",
      "name": "APP-745",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "source": {
      "id": "705",
      "name": "APP-317",
      "@type": "ReportingResource",
      "@referredType": "LogicalResource"
   },
   "@baseType": "Event",
   "@type": "CredentialStateChangeEvent"
```

```
}
```

# API OPERATIONS

Remember the following Uniform Contract:

| Operation on Entities | Uniform API Operation | Description |
|---|---|---|
| Query Entities | GET Resource | GET must be used to retrieve a representation of a resource. |
| Create Entity | POST Resource | POST must be used to create a new resource |
| Partial Update of an Entity | PATCH Resource | PATCH must be used to partially update a resource |
| Remove an Entity | DELETE Resource | DELETE must be used to remove a resource |
| Execute an Action on an Entity | POST on TASK Resource | POST must be used to execute Task Resources |
| Other Request Methods | POST on TASK Resource | GET and POST must not be used to tunnel other request methods. |

Filtering and attribute selection rules are described in the TMF REST Design Guidelines.

Notifications are also described in a subsequent section.

## Operations on DigitalIdentity

### Retrieves a DigitalIdentity by ID

`GET /digitalIdentity/{id}?fields=…`

#### Description

This operation retrieves a DigitalIdentity entity. Attribute selection is enabled for all first level attributes. Filtering may be available depending on the compliance level supported by an implementation.

#### Usage samples

Example of a request for retrieving a specific digital identity with id 2391ee4acbc142b1a4b74b4d4ab38152.

#### Request

```
GET /digitalIdentity/2391ee4acbc142b1a4b74b4d4ab38152
Content-Type: application/json
```

#### Response

```
200

{
   "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/digitalIdentity/2391ee4acbc142b1a4b74b4d4ab38152",
   "id": "2391ee4acbc142b1a4b74b4d4ab38152",
   "@type": "DigitalIdentity",
   "nickname": "Neo",
   "state": "Active",
   "validFor": {
      "startDateTime": "2018-09-21T23:20:50.52Z"
   },
   "credential": [
      {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/loginPasswordCredential/41af4b86e0b144cb9099b3d4c3a
b26ae",
         "id": "41af4b86e0b144cb9099b3d4c3ab26ae",
         "@type": "LoginPasswordCredential",
         "@baseType": "Credential",
         "state": "Active",
         "validFor": {
            "startDateTime": "2018-09-21T23:20:50.52Z"
         },
         "trustLevel": "high",
         "relatedContactMedium": [
            {
               "@type": "RelatedContactMedium",
               "role": "credential-login-alias-email",
               "contactMedium": {
                  "@type": "EmailContactMedium",
                  "@baseType": "ContactMedium",
                  "contactType": "private",
                  "id": "b2fe04a7f96e479195a47710abcf72be",
                  "preferred": true,
                  "validFor": {
                     "startDateTime": "2018-09-21T23:20:50.52Z"
                  },
                  "emailAddress": "neo@matrix.com"
               },
               "relationDate": "2018-09-21T23:20:50.52Z"
            },
            {
               "@type": "RelatedContactMedium",
               "role": "credential-login-alias-phone",
               "contactMedium": {
                  "@type": "PhoneContactMedium",
                  "@baseType": "ContactMedium",
                  "contactType": "private",
                  "id": "c0181f3d83e144a59162fd6136a98462",
                  "preferred": true,
                  "validFor": {
                     "startDateTime": "2018-09-21T23:20:50.52Z"
                  },
                  "phoneNumber": "+1 202-918-2132"
               },
               "relationDate": "2018-09-21T23:20:50.52Z"
            }
         ],
         "login": "neo1999",
         "creationDate": "2018-09-21T09:13:16-07:00",
         "lastUpdate": "2018-09-21T23:20:50.52Z"
```

```
      }
   ],
   "relatedContactMedium": [
      {
         "@type": "RelatedContactMedium",
         "role": "digital-id-recovery-email",
         "contactMedium": {
            "@type": "EmailContactMedium",
            "@baseType": "ContactMedium",
            "contactType": "private",
            "id": "b2fe04a7f96e479195a47710abcf72be",
            "preferred": true,
            "validFor": {
               "startDateTime": "2018-09-21T23:20:50.52Z"
            },
            "emailAddress": "neo@matrix.com"
         },
         "relationDate": "2018-09-21T23:20:50.52Z"
      },
      {
         "@type": "RelatedContactMedium",
         "role": "digital-id-recovery-phone",
         "contactMedium": {
            "@type": "PhoneContactMedium",
            "@baseType": "ContactMedium",
            "contactType": "private",
            "id": "60703a48038e4fc9a46bf1459aa3590f",
            "preferred": false,
            "validFor": {
               "startDateTime": "2018-09-21T23:20:50.52Z"
            },
            "phoneNumber": "+1 202-918-2132"
         },
         "relationDate": "2018-09-21T23:20:50.52Z"
      },
      {
         "@type": "RelatedContactMedium",
         "role": "digital-id-2nd-factor-phone",
         "contactMedium": {
            "@type": "PhoneContactMedium",
            "@baseType": "ContactMedium",
            "contactType": "private",
            "id": "c0181f3d83e144a59162fd6136a98462",
            "preferred": true,
            "validFor": {
               "startDateTime": "2018-09-21T23:20:50.52Z"
            },
            "phoneNumber": "+1 202-918-2132"
         },
         "relationDate": "2018-09-21T23:20:50.52Z"
      }
   ],
   "attachment": [
      {
         "@type": "Attachment",
         "attachmentType": "avatarPicture",
         "name": "Neo's avatar",
         "url": "https://i.pravatar.cc/150?u=neo",
         "mimeType": "image/jpeg",
         "size": {
            "amount": 91,
            "units": "Kb"
         },
```

```
            "validFor": {
               "startDateTime": "2018-09-21T23:20:50.52Z"
            }
         }
      ],
      "partyRoleIdentified": [
         {
            "@type": "RelatedSecurityPrincipalRef",
            "role": "Customer",
            "securityPrincipalRef": {
               "href": "https://serverRoot/tmf-
api/customerManagement/v5/partyRole/faa43dccaad142289e2b0f0e73e15958",
               "id": "faa43dccaad142289e2b0f0e73e15958",
               "@type": "PartyRoleRef",
               "@referredType": "PartyRole"
            }
         }
      ],
      "individualIdentified": {
         "href": "https://serverRoot/tmf-
api/partyManagement/v5/individual/193c8d6887394ca5b50290685db512ca",
         "id": "193c8d6887394ca5b50290685db512ca",
         "@type": "IndividualRef",
         "@referredType": "Individual"
      },
      "relatedSecurityPrincipal": [
         {
            "@type": "RelatedSecurityPrincipalRef",
            "role": "ServiceProvider",
            "securityPrincipalRef": {
               "href": "https://serverRoot/tmf-
api/partyManagement/v5/organization/e9b93f395a11453f9b7aa3349e857c24",
               "id": "e9b93f395a11453f9b7aa3349e857c24",
               "@type": "OrganizationRef",
               "@referredType": "Organization",
               "name": "Acme Inc."
            }
         },
         {
            "@type": "RelatedSecurityPrincipalRef",
            "role": "DigitalIdentityProvider",
            "securityPrincipalRef": {
               "href": "https://serverRoot/tmf-
api/partyManagement/v5/organization/af08cfda572749b0b4a90dfb75dfca51",
               "id": "af08cfda572749b0b4a90dfb75dfca51",
               "@type": "OrganizationRef",
               "@referredType": "Organization",
               "name": "Auth0"
            }
         }
      ],
      "creationDate": "2018-09-21T09:13:16-07:00",
      "lastUpdate": "2018-09-21T23:20:50.52Z"
   }
```


## List or find DigitalIdentity objects

### GET /digitalIdentity?fields=…

### Description

This operation list DigitalIdentity entities. Attribute selection is enabled for all first level attributes. Filtering may be available depending on the compliance level supported by an implementation.

### Usage samples

Example of a request for retrieving a list of digital identities in active state.

### Request

```
GET /digitalIdentity
Content-Type: application/json
```

### Response

```
200

[
   {
      "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/digitalIdentity/2391ee4acbc142b1a4b74b4d4ab38152",
      "id": "2391ee4acbc142b1a4b74b4d4ab38152",
      "@type": "DigitalIdentity",
      "nickname": "Neo",
      "state": "Active",
      "validFor": {
         "startDateTime": "2018-09-21T23:20:50.52Z"
      },
      "credential": [
         {
            "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/loginPasswordCredential/41af4b86e0b144cb9099b3d4c3a
b26ae",
            "id": "41af4b86e0b144cb9099b3d4c3ab26ae",
            "@type": "LoginPasswordCredential",
            "@baseType": "Credential",
            "state": "Active",
            "validFor": {
               "startDateTime": "2018-09-21T23:20:50.52Z"
            },
            "trustLevel": "high",
            "relatedContactMedium": [
               {
                  "@type": "RelatedContactMedium",
                  "role": "credential-login-alias-email",
                  "contactMedium": {
                     "@type": "EmailContactMedium",
                     "@baseType": "ContactMedium",
                     "contactType": "private",
                     "id": "b2fe04a7f96e479195a47710abcf72be",
                     "preferred": true,
                     "validFor": {
                        "startDateTime": "2018-09-21T23:20:50.52Z"
                     },
                     "emailAddress": "neo@matrix.com"
                  },
                  "relationDate": "2018-09-21T23:20:50.52Z"
               },
```

```
            {
               "@type": "RelatedContactMedium",
               "role": "credential-login-alias-phone",
               "contactMedium": {
                  "@type": "PhoneContactMedium",
                  "@baseType": "ContactMedium",
                  "contactType": "private",
                  "id": "c0181f3d83e144a59162fd6136a98462",
                  "preferred": true,
                  "validFor": {
                     "startDateTime": "2018-09-21T23:20:50.52Z"
                  },
                  "phoneNumber": "+1 202-918-2132"
               },
               "relationDate": "2018-09-21T23:20:50.52Z"
            }
         ],
         "login": "neo1999",
         "creationDate": "2018-09-21T09:13:16-07:00",
         "lastUpdate": "2018-09-21T23:20:50.52Z"
      }
   ],
   "relatedContactMedium": [
      {
         "@type": "RelatedContactMedium",
         "role": "digital-id-recovery-email",
         "contactMedium": {
            "@type": "EmailContactMedium",
            "@baseType": "ContactMedium",
            "contactType": "private",
            "id": "b2fe04a7f96e479195a47710abcf72be",
            "preferred": true,
            "validFor": {
               "startDateTime": "2018-09-21T23:20:50.52Z"
            },
            "emailAddress": "neo@matrix.com"
         },
         "relationDate": "2018-09-21T23:20:50.52Z"
      },
      {
         "@type": "RelatedContactMedium",
         "role": "digital-id-recovery-phone",
         "contactMedium": {
            "@type": "PhoneContactMedium",
            "@baseType": "ContactMedium",
            "contactType": "private",
            "id": "60703a48038e4fc9a46bf1459aa3590f",
            "preferred": false,
            "validFor": {
               "startDateTime": "2018-09-21T23:20:50.52Z"
            },
            "phoneNumber": "+1 202-918-2132"
         },
         "relationDate": "2018-09-21T23:20:50.52Z"
      },
      {
         "@type": "RelatedContactMedium",
         "role": "digital-id-2nd-factor-phone",
         "contactMedium": {
            "@type": "PhoneContactMedium",
            "@baseType": "ContactMedium",
            "contactType": "private",
            "id": "c0181f3d83e144a59162fd6136a98462",
```

```
               "preferred": true,
               "validFor": {
                  "startDateTime": "2018-09-21T23:20:50.52Z"
               },
               "phoneNumber": "+1 202-918-2132"
            },
            "relationDate": "2018-09-21T23:20:50.52Z"
         }
      ],
      "attachment": [
         {
            "@type": "Attachment",
            "attachmentType": "avatarPicture",
            "name": "Neo's avatar",
            "url": "https://i.pravatar.cc/150?u=neo",
            "mimeType": "image/jpeg",
            "size": {
               "amount": 91,
               "units": "Kb"
            },
            "validFor": {
               "startDateTime": "2018-09-21T23:20:50.52Z"
            }
         }
      ],
      "partyRoleIdentified": [
         {
            "@type": "RelatedSecurityPrincipalRef",
            "role": "Customer",
            "securityPrincipalRef": {
               "href": "https://serverRoot/tmf-
api/customerManagement/v5/partyRole/faa43dccaad142289e2b0f0e73e15958",
               "id": "faa43dccaad142289e2b0f0e73e15958",
               "@type": "PartyRoleRef",
               "@referredType": "PartyRole"
            }
         }
      ],
      "individualIdentified": {
         "href": "https://serverRoot/tmf-
api/partyManagement/v5/individual/193c8d6887394ca5b50290685db512ca",
         "id": "193c8d6887394ca5b50290685db512ca",
         "@type": "IndividualRef",
         "@referredType": "Individual"
      },
      "relatedSecurityPrincipal": [
         {
            "@type": "RelatedSecurityPrincipalRef",
            "role": "ServiceProvider",
            "securityPrincipalRef": {
               "href": "https://serverRoot/tmf-
api/partyManagement/v5/organization/e9b93f395a11453f9b7aa3349e857c24",
               "id": "e9b93f395a11453f9b7aa3349e857c24",
               "@type": "OrganizationRef",
               "@referredType": "Organization",
               "name": "Acme Inc."
            }
         },
         {
            "@type": "RelatedSecurityPrincipalRef",
            "role": "DigitalIdentityProvider",
            "securityPrincipalRef": {
               "href": "https://serverRoot/tmf-
```

```
api/partyManagement/v5/organization/af08cfda572749b0b4a90dfb75dfca51",
                "id": "af08cfda572749b0b4a90dfb75dfca51",
                "@type": "OrganizationRef",
                "@referredType": "Organization",
                "name": "Auth0"
            }
         }
      ],
      "creationDate": "2018-09-21T09:13:16-07:00",
      "lastUpdate": "2018-09-21T23:20:50.52Z"
   }
]
```

## Creates a DigitalIdentity

### POST /digitalIdentity?fields=…

#### Description

This operation creates a DigitalIdentity entity.

#### Mandatory Attributes

| Mandatory Attributes | Rule |
|---|---|
| credential | |
| credential.@type | |
| credential.id | |
| credential.state | |
| credential.trustLevel | |
| credential.validFor | |
| id | |
| state | |
| validFor | |
| @type | |

#### Usage samples

Creation of a new digital identity with POST operation.

#### Request

```
POST /digitalIdentity
Content-Type: application/json

{
   "@type": "DigitalIdentity",
   "nickname": "Neo",
   "state": "Active",
   "validFor": {
```

```
        "startDateTime": "2018-09-21T23:20:50.52Z"
    },
    "credential": [
        {
            "@type": "LoginPasswordCredential",
            "@baseType": "Credential",
            "relatedContactMedium": [
                {
                    "@type": "RelatedContactMedium",
                    "role": "credential-login-alias-email",
                    "contactMedium": {
                        "@type": "EmailContactMedium",
                        "@baseType": "ContactMedium",
                        "contactType": "private",
                        "id": "b2fe04a7f96e479195a47710abcf72be",
                        "preferred": true,
                        "validFor": {
                            "startDateTime": "2018-09-21T23:20:50.52Z"
                        },
                        "emailAddress": "neo@matrix.com"
                    },
                    "relationDate": "2018-09-21T23:20:50.52Z"
                },
                {
                    "@type": "RelatedContactMedium",
                    "role": "credential-login-alias-phone",
                    "contactMedium": {
                        "@type": "PhoneContactMedium",
                        "@baseType": "ContactMedium",
                        "contactType": "private",
                        "id": "c0181f3d83e144a59162fd6136a98462",
                        "preferred": true,
                        "validFor": {
                            "startDateTime": "2018-09-21T23:20:50.52Z"
                        },
                        "phoneNumber": "+1 202-918-2132"
                    },
                    "relationDate": "2018-09-21T23:20:50.52Z"
                }
            ],
            "login": "neo1999",
            "password": "*******"
        }
    ],
    "relatedContactMedium": [
        {
            "@type": "RelatedContactMedium",
            "role": "digital-id-recovery-email",
            "contactMedium": {
                "@type": "EmailContactMedium",
                "@baseType": "ContactMedium",
                "contactType": "private",
                "id": "b2fe04a7f96e479195a47710abcf72be",
                "preferred": true,
                "validFor": {
                    "startDateTime": "2018-09-21T23:20:50.52Z"
                },
                "emailAddress": "neo@matrix.com"
            },
            "relationDate": "2018-09-21T23:20:50.52Z"
        },
        {
            "@type": "RelatedContactMedium",
```

```
            "role": "digital-id-recovery-phone",
            "contactMedium": {
               "@type": "PhoneContactMedium",
               "@baseType": "ContactMedium",
               "contactType": "private",
               "id": "60703a48038e4fc9a46bf1459aa3590f",
               "preferred": false,
               "validFor": {
                  "startDateTime": "2018-09-21T23:20:50.52Z"
               },
               "phoneNumber": "+1 202-918-2132"
            },
            "relationDate": "2018-09-21T23:20:50.52Z"
         },
         {
            "@type": "RelatedContactMedium",
            "role": "digital-id-2nd-factor-phone",
            "contactMedium": {
               "@type": "PhoneContactMedium",
               "@baseType": "ContactMedium",
               "contactType": "private",
               "id": "c0181f3d83e144a59162fd6136a98462",
               "preferred": true,
               "validFor": {
                  "startDateTime": "2018-09-21T23:20:50.52Z"
               },
               "phoneNumber": "+1 202-918-2132"
            },
            "relationDate": "2018-09-21T23:20:50.52Z"
         }
      ],
      "attachment": [
         {
            "@type": "Attachment",
            "attachmentType": "avatarPicture",
            "name": "Neo's avatar",
            "url": "https://i.pravatar.cc/150?u=neo",
            "mimeType": "image/jpeg",
            "size": {
               "amount": 91,
               "units": "Kb"
            },
            "validFor": {
               "startDateTime": "2018-09-21T23:20:50.52Z"
            }
         }
      ],
      "partyRoleIdentified": [
         {
            "@type": "RelatedSecurityPrincipalRef",
            "role": "Customer",
            "securityPrincipalRef": {
               "href": "https://serverRoot/tmf-
   api/customerManagement/v5/partyRole/faa43dccaad142289e2b0f0e73e15958",
               "id": "faa43dccaad142289e2b0f0e73e15958",
               "@type": "PartyRoleRef",
               "@referredType": "PartyRole"
            }
         }
      ],
      "individualIdentified": {
         "href": "https://serverRoot/tmf-
   api/partyManagement/v5/individual/193c8d6887394ca5b50290685db512ca",
```

```
      "id": "193c8d6887394ca5b50290685db512ca",
      "@type": "IndividualRef",
      "@referredType": "Individual"
   },
   "relatedSecurityPrincipal": [
      {
         "@type": "RelatedSecurityPrincipalRef",
         "role": "ServiceProvider",
         "securityPrincipalRef": {
            "href": "https://serverRoot/tmf-
api/partyManagement/v5/organization/e9b93f395a11453f9b7aa3349e857c24",
            "id": "e9b93f395a11453f9b7aa3349e857c24",
            "@type": "OrganizationRef",
            "@referredType": "Organization",
            "name": "Acme Inc."
         }
      },
      {
         "@type": "RelatedSecurityPrincipalRef",
         "role": "DigitalIdentityProvider",
         "securityPrincipalRef": {
            "href": "https://serverRoot/tmf-
api/partyManagement/v5/organization/af08cfda572749b0b4a90dfb75dfca51",
            "id": "af08cfda572749b0b4a90dfb75dfca51",
            "@type": "OrganizationRef",
            "@referredType": "Organization",
            "name": "Auth0"
         }
      }
   ]
}
```


## Response


```
201

{
   "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/digitalIdentity/2391ee4acbc142b1a4b74b4d4ab38152",
   "id": "2391ee4acbc142b1a4b74b4d4ab38152",
   "@type": "DigitalIdentity",
   "nickname": "Neo",
   "state": "Active",
   "validFor": {
      "startDateTime": "2018-09-21T23:20:50.52Z"
   },
   "credential": [
      {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/loginPasswordCredential/41af4b86e0b144cb9099b3d4c3a
b26ae",
         "id": "41af4b86e0b144cb9099b3d4c3ab26ae",
         "@type": "LoginPasswordCredential",
         "@baseType": "Credential",
         "state": "Active",
         "validFor": {
            "startDateTime": "2018-09-21T23:20:50.52Z"
         },
         "trustLevel": "high",
         "relatedContactMedium": [
```

```
            {
               "@type": "RelatedContactMedium",
               "role": "credential-login-alias-email",
               "contactMedium": {
                  "@type": "EmailContactMedium",
                  "@baseType": "ContactMedium",
                  "contactType": "private",
                  "id": "b2fe04a7f96e479195a47710abcf72be",
                  "preferred": true,
                  "validFor": {
                     "startDateTime": "2018-09-21T23:20:50.52Z"
                  },
                  "emailAddress": "neo@matrix.com"
               },
               "relationDate": "2018-09-21T23:20:50.52Z"
            },
            {
               "@type": "RelatedContactMedium",
               "role": "credential-login-alias-phone",
               "contactMedium": {
                  "@type": "PhoneContactMedium",
                  "@baseType": "ContactMedium",
                  "contactType": "private",
                  "id": "c0181f3d83e144a59162fd6136a98462",
                  "preferred": true,
                  "validFor": {
                     "startDateTime": "2018-09-21T23:20:50.52Z"
                  },
                  "phoneNumber": "+1 202-918-2132"
               },
               "relationDate": "2018-09-21T23:20:50.52Z"
            }
         ],
         "login": "neo1999",
         "creationDate": "2018-09-21T09:13:16-07:00",
         "lastUpdate": "2018-09-21T23:20:50.52Z"
      }
   ],
   "relatedContactMedium": [
      {
         "@type": "RelatedContactMedium",
         "role": "digital-id-recovery-email",
         "contactMedium": {
            "@type": "EmailContactMedium",
            "@baseType": "ContactMedium",
            "contactType": "private",
            "id": "b2fe04a7f96e479195a47710abcf72be",
            "preferred": true,
            "validFor": {
               "startDateTime": "2018-09-21T23:20:50.52Z"
            },
            "emailAddress": "neo@matrix.com"
         },
         "relationDate": "2018-09-21T23:20:50.52Z"
      },
      {
         "@type": "RelatedContactMedium",
         "role": "digital-id-recovery-phone",
         "contactMedium": {
            "@type": "PhoneContactMedium",
            "@baseType": "ContactMedium",
            "contactType": "private",
            "id": "60703a48038e4fc9a46bf1459aa3590f",
```

```
            "preferred": false,
            "validFor": {
               "startDateTime": "2018-09-21T23:20:50.52Z"
            },
            "phoneNumber": "+1 202-918-2132"
         },
         "relationDate": "2018-09-21T23:20:50.52Z"
      },
      {
         "@type": "RelatedContactMedium",
         "role": "digital-id-2nd-factor-phone",
         "contactMedium": {
            "@type": "PhoneContactMedium",
            "@baseType": "ContactMedium",
            "contactType": "private",
            "id": "c0181f3d83e144a59162fd6136a98462",
            "preferred": true,
            "validFor": {
               "startDateTime": "2018-09-21T23:20:50.52Z"
            },
            "phoneNumber": "+1 202-918-2132"
         },
         "relationDate": "2018-09-21T23:20:50.52Z"
      }
   ],
   "attachment": [
      {
         "@type": "Attachment",
         "attachmentType": "avatarPicture",
         "name": "Neo's avatar",
         "url": "https://i.pravatar.cc/150?u=neo",
         "mimeType": "image/jpeg",
         "size": {
            "amount": 91,
            "units": "Kb"
         },
         "validFor": {
            "startDateTime": "2018-09-21T23:20:50.52Z"
         }
      }
   ],
   "partyRoleIdentified": [
      {
         "@type": "RelatedSecurityPrincipalRef",
         "role": "Customer",
         "securityPrincipalRef": {
            "href": "https://serverRoot/tmf-
api/customerManagement/v5/partyRole/faa43dccaad142289e2b0f0e73e15958",
            "id": "faa43dccaad142289e2b0f0e73e15958",
            "@type": "PartyRoleRef",
            "@referredType": "PartyRole"
         }
      }
   ],
   "individualIdentified": {
      "href": "https://serverRoot/tmf-
api/partyManagement/v5/individual/193c8d6887394ca5b50290685db512ca",
      "id": "193c8d6887394ca5b50290685db512ca",
      "@type": "IndividualRef",
      "@referredType": "Individual"
   },
   "relatedSecurityPrincipal": [
      {
```

```
         "@type": "RelatedSecurityPrincipalRef",
         "role": "ServiceProvider",
         "securityPrincipalRef": {
            "href": "https://serverRoot/tmf-
api/partyManagement/v5/organization/e9b93f395a11453f9b7aa3349e857c24",
            "id": "e9b93f395a11453f9b7aa3349e857c24",
            "@type": "OrganizationRef",
            "@referredType": "Organization",
            "name": "Acme Inc."
         }
      },
      {
         "@type": "RelatedSecurityPrincipalRef",
         "role": "DigitalIdentityProvider",
         "securityPrincipalRef": {
            "href": "https://serverRoot/tmf-
api/partyManagement/v5/organization/af08cfda572749b0b4a90dfb75dfca51",
            "id": "af08cfda572749b0b4a90dfb75dfca51",
            "@type": "OrganizationRef",
            "@referredType": "Organization",
            "name": "Auth0"
         }
      }
   ],
   "creationDate": "2018-09-21T09:13:16-07:00",
   "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```


## Updates partially a DigitalIdentity

**`PATCH /digitalIdentity/{id}?fields=…`**

### Description

This operation allows partial updates of a DigitalIdentity entity. Support of json/merge (https://tools.ietf.org/html/rfc7396) is mandatory, support of json/patch (http://tools.ietf.org/html/rfc5789) is optional. Note: If the update operation yields to the creation of sub-resources or relationships, the same rules concerning mandatory sub-resource attributes and default value settings in the POST operation applies to the PATCH operation. Hence these tables are not repeated here.

### Patchable and Non Patchable Attributes

| Non Patchable Attributes | Rule |
|---|---|
| creationDate | |
| href | |
| id | |
| @baseType | @baseType is immutable |
| @schemaLocation | @schemaLocation is immutable |
| @type | @type is immutable |

| Patchable Attributes | Rule |
|---|---|
| attachment | |
| credential | |
| individualIdentified | |
| lastUpdate | |
| nickname | |
| partyRoleIdentified | |
| relatedContactMedium | |
| relatedSecurityPrincipal | |
| resourceIdentified | |
| resourceRoleIdentified | |
| state | |
| validFor | |

### Usage samples

Example of a request for fully updating an entire digital identity.

### Request

```
PATCH /digitalIdentity/2391ee4acbc142b1a4b74b4d4ab38152
Content-Type: application/json

{
   "@type": "DigitalIdentity",
   "nickname": "Neo",
   "individualIdentified": {
      "id": "193c8d6887394ca5b50290685db512ca",
      "@type": "IndividualRef",
      "@referredType": "Individual"
   }

}
```

### Response

```
200

{
   "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/digitalIdentity/2391ee4acbc142b1a4b74b4d4ab38152",
   "id": "2391ee4acbc142b1a4b74b4d4ab38152",
   "@type": "DigitalIdentity",
   "nickname": "Neo",
   "state": "Active",
   "validFor": {
      "startDateTime": "2018-09-21T23:20:50.52Z"
   },
```

```
    "credential": [
       {
          "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/loginPasswordCredential/41af4b86e0b144cb9099b3d4c3a
b26ae",
          "id": "41af4b86e0b144cb9099b3d4c3ab26ae",
          "@type": "LoginPasswordCredential",
          "@baseType": "Credential",
          "state": "Active",
          "validFor": {
             "startDateTime": "2018-09-21T23:20:50.52Z"
          },
          "trustLevel": "high",
          "relatedContactMedium": [
             {
                "@type": "RelatedContactMedium",
                "role": "credential-login-alias-email",
                "contactMedium": {
                   "@type": "EmailContactMedium",
                   "@baseType": "ContactMedium",
                   "contactType": "private",
                   "id": "b2fe04a7f96e479195a47710abcf72be",
                   "preferred": true,
                   "validFor": {
                      "startDateTime": "2018-09-21T23:20:50.52Z"
                   },
                   "emailAddress": "neo@matrix.com"
                },
                "relationDate": "2018-09-21T23:20:50.52Z"
             },
             {
                "@type": "RelatedContactMedium",
                "role": "credential-login-alias-phone",
                "contactMedium": {
                   "@type": "PhoneContactMedium",
                   "@baseType": "ContactMedium",
                   "contactType": "private",
                   "id": "c0181f3d83e144a59162fd6136a98462",
                   "preferred": true,
                   "validFor": {
                      "startDateTime": "2018-09-21T23:20:50.52Z"
                   },
                   "phoneNumber": "+1 202-918-2132"
                },
                "relationDate": "2018-09-21T23:20:50.52Z"
             }
          ],
          "login": "neo1999",
          "creationDate": "2018-09-21T09:13:16-07:00",
          "lastUpdate": "2018-09-21T23:20:50.52Z"
       }
    ],
    "relatedContactMedium": [
       {
          "@type": "RelatedContactMedium",
          "role": "digital-id-recovery-email",
          "contactMedium": {
             "@type": "EmailContactMedium",
             "@baseType": "ContactMedium",
             "contactType": "private",
             "id": "b2fe04a7f96e479195a47710abcf72be",
             "preferred": true,
             "validFor": {
```

```
                "startDateTime": "2018-09-21T23:20:50.52Z"
             },
             "emailAddress": "neo@matrix.com"
          },
          "relationDate": "2018-09-21T23:20:50.52Z"
       },
       {
          "@type": "RelatedContactMedium",
          "role": "digital-id-recovery-phone",
          "contactMedium": {
             "@type": "PhoneContactMedium",
             "@baseType": "ContactMedium",
             "contactType": "private",
             "id": "60703a48038e4fc9a46bf1459aa3590f",
             "preferred": false,
             "validFor": {
                "startDateTime": "2018-09-21T23:20:50.52Z"
             },
             "phoneNumber": "+1 202-918-2132"
          },
          "relationDate": "2018-09-21T23:20:50.52Z"
       },
       {
          "@type": "RelatedContactMedium",
          "role": "digital-id-2nd-factor-phone",
          "contactMedium": {
             "@type": "PhoneContactMedium",
             "@baseType": "ContactMedium",
             "contactType": "private",
             "id": "c0181f3d83e144a59162fd6136a98462",
             "preferred": true,
             "validFor": {
                "startDateTime": "2018-09-21T23:20:50.52Z"
             },
             "phoneNumber": "+1 202-918-2132"
          },
          "relationDate": "2018-09-21T23:20:50.52Z"
       }
    ],
    "attachment": [
       {
          "@type": "Attachment",
          "attachmentType": "avatarPicture",
          "name": "Neo's avatar",
          "url": "https://i.pravatar.cc/150?u=neo",
          "mimeType": "image/jpeg",
          "size": {
             "amount": 91,
             "units": "Kb"
          },
          "validFor": {
             "startDateTime": "2018-09-21T23:20:50.52Z"
          }
       }
    ],
    "partyRoleIdentified": [
       {
          "@type": "RelatedSecurityPrincipalRef",
          "role": "Customer",
          "securityPrincipalRef": {
             "href": "https://serverRoot/tmf-
api/customerManagement/v5/partyRole/faa43dccaad142289e2b0f0e73e15958",
             "id": "faa43dccaad142289e2b0f0e73e15958",
```

```
            "@type": "PartyRoleRef",
            "@referredType": "PartyRole"
         }
      }
   ],
   "individualIdentified": {
      "href": "https://serverRoot/tmf-
api/partyManagement/v5/individual/193c8d6887394ca5b50290685db512ca",
      "id": "193c8d6887394ca5b50290685db512ca",
      "@type": "IndividualRef",
      "@referredType": "Individual"
   },
   "relatedSecurityPrincipal": [
      {
         "@type": "RelatedSecurityPrincipalRef",
         "role": "ServiceProvider",
         "securityPrincipalRef": {
            "href": "https://serverRoot/tmf-
api/partyManagement/v5/organization/e9b93f395a11453f9b7aa3349e857c24",
            "id": "e9b93f395a11453f9b7aa3349e857c24",
            "@type": "OrganizationRef",
            "@referredType": "Organization",
            "name": "Acme Inc."
         }
      },
      {
         "@type": "RelatedSecurityPrincipalRef",
         "role": "DigitalIdentityProvider",
         "securityPrincipalRef": {
            "href": "https://serverRoot/tmf-
api/partyManagement/v5/organization/af08cfda572749b0b4a90dfb75dfca51",
            "id": "af08cfda572749b0b4a90dfb75dfca51",
            "@type": "OrganizationRef",
            "@referredType": "Organization",
            "name": "Auth0"
         }
      }
   ],
   "creationDate": "2018-09-21T09:13:16-07:00",
   "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```


Example of a request for partial updating a digital identity, using MERGE Patch.

**Request**

```
PATCH /digitalIdentity/2391ee4acbc142b1a4b74b4d4ab38152
Content-Type: application/merge-patch+json

{
   "@type": "DigitalIdentity",
   "nickname": "Neo",
   "individualIdentified": {
      "id": "193c8d6887394ca5b50290685db512ca",
      "@type": "IndividualRef",
      "@referredType": "Individual"
   }

}
```

### Response


```
200

{
   "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/digitalIdentity/2391ee4acbc142b1a4b74b4d4ab38152",
   "id": "2391ee4acbc142b1a4b74b4d4ab38152",
   "@type": "DigitalIdentity",
   "nickname": "Neo",
   "state": "Active",
   "validFor": {
      "startDateTime": "2018-09-21T23:20:50.52Z"
   },
   "credential": [
      {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/loginPasswordCredential/41af4b86e0b144cb9099b3d4c3a
b26ae",
         "id": "41af4b86e0b144cb9099b3d4c3ab26ae",
         "@type": "LoginPasswordCredential",
         "@baseType": "Credential",
         "state": "Active",
         "validFor": {
            "startDateTime": "2018-09-21T23:20:50.52Z"
         },
         "trustLevel": "high",
         "relatedContactMedium": [
            {
               "@type": "RelatedContactMedium",
               "role": "credential-login-alias-email",
               "contactMedium": {
                  "@type": "EmailContactMedium",
                  "@baseType": "ContactMedium",
                  "contactType": "private",
                  "id": "b2fe04a7f96e479195a47710abcf72be",
                  "preferred": true,
                  "validFor": {
                     "startDateTime": "2018-09-21T23:20:50.52Z"
                  },
                  "emailAddress": "neo@matrix.com"
               },
               "relationDate": "2018-09-21T23:20:50.52Z"
            },
            {
               "@type": "RelatedContactMedium",
               "role": "credential-login-alias-phone",
               "contactMedium": {
                  "@type": "PhoneContactMedium",
                  "@baseType": "ContactMedium",
                  "contactType": "private",
                  "id": "c0181f3d83e144a59162fd6136a98462",
                  "preferred": true,
                  "validFor": {
                     "startDateTime": "2018-09-21T23:20:50.52Z"
                  },
                  "phoneNumber": "+1 202-918-2132"
               },
               "relationDate": "2018-09-21T23:20:50.52Z"
            }
         ],
```

```
            "login": "neo1999",
            "creationDate": "2018-09-21T09:13:16-07:00",
            "lastUpdate": "2018-09-21T23:20:50.52Z"
         }
      ],
      "relatedContactMedium": [
         {
            "@type": "RelatedContactMedium",
            "role": "digital-id-recovery-email",
            "contactMedium": {
               "@type": "EmailContactMedium",
               "@baseType": "ContactMedium",
               "contactType": "private",
               "id": "b2fe04a7f96e479195a47710abcf72be",
               "preferred": true,
               "validFor": {
                  "startDateTime": "2018-09-21T23:20:50.52Z"
               },
               "emailAddress": "neo@matrix.com"
            },
            "relationDate": "2018-09-21T23:20:50.52Z"
         },
         {
            "@type": "RelatedContactMedium",
            "role": "digital-id-recovery-phone",
            "contactMedium": {
               "@type": "PhoneContactMedium",
               "@baseType": "ContactMedium",
               "contactType": "private",
               "id": "60703a48038e4fc9a46bf1459aa3590f",
               "preferred": false,
               "validFor": {
                  "startDateTime": "2018-09-21T23:20:50.52Z"
               },
               "phoneNumber": "+1 202-918-2132"
            },
            "relationDate": "2018-09-21T23:20:50.52Z"
         },
         {
            "@type": "RelatedContactMedium",
            "role": "digital-id-2nd-factor-phone",
            "contactMedium": {
               "@type": "PhoneContactMedium",
               "@baseType": "ContactMedium",
               "contactType": "private",
               "id": "c0181f3d83e144a59162fd6136a98462",
               "preferred": true,
               "validFor": {
                  "startDateTime": "2018-09-21T23:20:50.52Z"
               },
               "phoneNumber": "+1 202-918-2132"
            },
            "relationDate": "2018-09-21T23:20:50.52Z"
         }
      ],
      "attachment": [
         {
            "@type": "Attachment",
            "attachmentType": "avatarPicture",
            "name": "Neo's avatar",
            "url": "https://i.pravatar.cc/150?u=neo",
            "mimeType": "image/jpeg",
            "size": {
```

```
            "amount": 91,
            "units": "Kb"
         },
         "validFor": {
            "startDateTime": "2018-09-21T23:20:50.52Z"
         }
      }
   ],
   "partyRoleIdentified": [
      {
         "@type": "RelatedSecurityPrincipalRef",
         "role": "Customer",
         "securityPrincipalRef": {
            "href": "https://serverRoot/tmf-
api/customerManagement/v5/partyRole/faa43dccaad142289e2b0f0e73e15958",
            "id": "faa43dccaad142289e2b0f0e73e15958",
            "@type": "PartyRoleRef",
            "@referredType": "PartyRole"
         }
      }
   ],
   "individualIdentified": {
      "href": "https://serverRoot/tmf-
api/partyManagement/v5/individual/193c8d6887394ca5b50290685db512ca",
      "id": "193c8d6887394ca5b50290685db512ca",
      "@type": "IndividualRef",
      "@referredType": "Individual"
   },
   "relatedSecurityPrincipal": [
      {
         "@type": "RelatedSecurityPrincipalRef",
         "role": "ServiceProvider",
         "securityPrincipalRef": {
            "href": "https://serverRoot/tmf-
api/partyManagement/v5/organization/e9b93f395a11453f9b7aa3349e857c24",
            "id": "e9b93f395a11453f9b7aa3349e857c24",
            "@type": "OrganizationRef",
            "@referredType": "Organization",
            "name": "Acme Inc."
         }
      },
      {
         "@type": "RelatedSecurityPrincipalRef",
         "role": "DigitalIdentityProvider",
         "securityPrincipalRef": {
            "href": "https://serverRoot/tmf-
api/partyManagement/v5/organization/af08cfda572749b0b4a90dfb75dfca51",
            "id": "af08cfda572749b0b4a90dfb75dfca51",
            "@type": "OrganizationRef",
            "@referredType": "Organization",
            "name": "Auth0"
         }
      }
   ],
   "creationDate": "2018-09-21T09:13:16-07:00",
   "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```


Example of a request for partial updating a digital identity, using JSON Patch.

### Request

```
PATCH /digitalIdentity/2391ee4acbc142b1a4b74b4d4ab38152
Content-Type: application/json-patch+json

[
  {
    "op": "replace",
    "path": "/nickame",
    "value": "Neo"
  },
  {
    "op": "replace",
    "path": "/login",
    "value": "neo1999"
  },
  {
    "op": "replace",
    "path": "/password",
    "value": "KB8ppUDg4DqcXtbX2Xb97c4RSqvBPPuH"
  }
]
```

### Response

```
200

{
   "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/digitalIdentity/2391ee4acbc142b1a4b74b4d4ab38152",
   "id": "2391ee4acbc142b1a4b74b4d4ab38152",
   "@type": "DigitalIdentity",
   "nickname": "Neo",
   "state": "Active",
   "validFor": {
      "startDateTime": "2018-09-21T23:20:50.52Z"
   },
   "credential": [
      {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/loginPasswordCredential/41af4b86e0b144cb9099b3d4c3a
b26ae",
         "id": "41af4b86e0b144cb9099b3d4c3ab26ae",
         "@type": "LoginPasswordCredential",
         "@baseType": "Credential",
         "state": "Active",
         "validFor": {
            "startDateTime": "2018-09-21T23:20:50.52Z"
         },
         "trustLevel": "high",
         "relatedContactMedium": [
            {
               "@type": "RelatedContactMedium",
               "role": "credential-login-alias-email",
               "contactMedium": {
                  "@type": "EmailContactMedium",
                  "@baseType": "ContactMedium",
                  "contactType": "private",
                  "id": "b2fe04a7f96e479195a47710abcf72be",
                  "preferred": true,
                  "validFor": {
```

```
                    "startDateTime": "2018-09-21T23:20:50.52Z"
                 },
                 "emailAddress": "neo@matrix.com"
              },
              "relationDate": "2018-09-21T23:20:50.52Z"
           },
           {
              "@type": "RelatedContactMedium",
              "role": "credential-login-alias-phone",
              "contactMedium": {
                 "@type": "PhoneContactMedium",
                 "@baseType": "ContactMedium",
                 "contactType": "private",
                 "id": "c0181f3d83e144a59162fd6136a98462",
                 "preferred": true,
                 "validFor": {
                    "startDateTime": "2018-09-21T23:20:50.52Z"
                 },
                 "phoneNumber": "+1 202-918-2132"
              },
              "relationDate": "2018-09-21T23:20:50.52Z"
           }
        ],
        "login": "neo1999",
        "creationDate": "2018-09-21T09:13:16-07:00",
        "lastUpdate": "2018-09-21T23:20:50.52Z"
     }
  ],
  "relatedContactMedium": [
     {
        "@type": "RelatedContactMedium",
        "role": "digital-id-recovery-email",
        "contactMedium": {
           "@type": "EmailContactMedium",
           "@baseType": "ContactMedium",
           "contactType": "private",
           "id": "b2fe04a7f96e479195a47710abcf72be",
           "preferred": true,
           "validFor": {
              "startDateTime": "2018-09-21T23:20:50.52Z"
           },
           "emailAddress": "neo@matrix.com"
        },
        "relationDate": "2018-09-21T23:20:50.52Z"
     },
     {
        "@type": "RelatedContactMedium",
        "role": "digital-id-recovery-phone",
        "contactMedium": {
           "@type": "PhoneContactMedium",
           "@baseType": "ContactMedium",
           "contactType": "private",
           "id": "60703a48038e4fc9a46bf1459aa3590f",
           "preferred": false,
           "validFor": {
              "startDateTime": "2018-09-21T23:20:50.52Z"
           },
           "phoneNumber": "+1 202-918-2132"
        },
        "relationDate": "2018-09-21T23:20:50.52Z"
     },
     {
        "@type": "RelatedContactMedium",
```

```
         "role": "digital-id-2nd-factor-phone",
         "contactMedium": {
            "@type": "PhoneContactMedium",
            "@baseType": "ContactMedium",
            "contactType": "private",
            "id": "c0181f3d83e144a59162fd6136a98462",
            "preferred": true,
            "validFor": {
               "startDateTime": "2018-09-21T23:20:50.52Z"
            },
            "phoneNumber": "+1 202-918-2132"
         },
         "relationDate": "2018-09-21T23:20:50.52Z"
      }
   ],
   "attachment": [
      {
         "@type": "Attachment",
         "attachmentType": "avatarPicture",
         "name": "Neo's avatar",
         "url": "https://i.pravatar.cc/150?u=neo",
         "mimeType": "image/jpeg",
         "size": {
            "amount": 91,
            "units": "Kb"
         },
         "validFor": {
            "startDateTime": "2018-09-21T23:20:50.52Z"
         }
      }
   ],
   "partyRoleIdentified": [
      {
         "@type": "RelatedSecurityPrincipalRef",
         "role": "Customer",
         "securityPrincipalRef": {
            "href": "https://serverRoot/tmf-
api/customerManagement/v5/partyRole/faa43dccaad142289e2b0f0e73e15958",
            "id": "faa43dccaad142289e2b0f0e73e15958",
            "@type": "PartyRoleRef",
            "@referredType": "PartyRole"
         }
      }
   ],
   "individualIdentified": {
      "href": "https://serverRoot/tmf-
api/partyManagement/v5/individual/193c8d6887394ca5b50290685db512ca",
      "id": "193c8d6887394ca5b50290685db512ca",
      "@type": "IndividualRef",
      "@referredType": "Individual"
   },
   "relatedSecurityPrincipal": [
      {
         "@type": "RelatedSecurityPrincipalRef",
         "role": "ServiceProvider",
         "securityPrincipalRef": {
            "href": "https://serverRoot/tmf-
api/partyManagement/v5/organization/e9b93f395a11453f9b7aa3349e857c24",
            "id": "e9b93f395a11453f9b7aa3349e857c24",
            "@type": "OrganizationRef",
            "@referredType": "Organization",
            "name": "Acme Inc."
         }
```

```
      },
      {
         "@type": "RelatedSecurityPrincipalRef",
         "role": "DigitalIdentityProvider",
         "securityPrincipalRef": {
            "href": "https://serverRoot/tmf-
api/partyManagement/v5/organization/af08cfda572749b0b4a90dfb75dfca51",
            "id": "af08cfda572749b0b4a90dfb75dfca51",
            "@type": "OrganizationRef",
            "@referredType": "Organization",
            "name": "Auth0"
         }
      }
   ],
   "creationDate": "2018-09-21T09:13:16-07:00",
   "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```

Example of a request for partial updating a digital identity, using JSON Patch Query.

### Request

```
PATCH /digitalIdentity/2391ee4acbc142b1a4b74b4d4ab38152
Content-Type: application/json-patch-query+json

[
  {
    "op": "replace",
    "path": "/contactMedium?contactMedium.id=b2fe04a7f96e479195a47710abcf72be",
    "value": {
      "@type": "DigitalIdentityContactMedium",
      "@baseType": "ContactMedium",
      "@referredType": "EmailContactMedium",
      "contactType": "private",
      "id": "b2fe04a7f96e479195a47710abcf72be",
      "preferred": true,
      "validFor": {
        "startDateTime": "2018-09-21T23:20:50.52Z"
      },
      "emailAddress": "neo@matrix.com",
      "role": "password_reset_email_contact"
    }
  }
]
```

### Response

```
200

{
   "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/digitalIdentity/2391ee4acbc142b1a4b74b4d4ab38152",
   "id": "2391ee4acbc142b1a4b74b4d4ab38152",
   "@type": "DigitalIdentity",
   "nickname": "Neo",
   "state": "Active",
   "validFor": {
```

```
      "startDateTime": "2018-09-21T23:20:50.52Z"
   },
   "credential": [
      {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/loginPasswordCredential/41af4b86e0b144cb9099b3d4c3a
b26ae",
         "id": "41af4b86e0b144cb9099b3d4c3ab26ae",
         "@type": "LoginPasswordCredential",
         "@baseType": "Credential",
         "state": "Active",
         "validFor": {
            "startDateTime": "2018-09-21T23:20:50.52Z"
         },
         "trustLevel": "high",
         "relatedContactMedium": [
            {
               "@type": "RelatedContactMedium",
               "role": "credential-login-alias-email",
               "contactMedium": {
                  "@type": "EmailContactMedium",
                  "@baseType": "ContactMedium",
                  "contactType": "private",
                  "id": "b2fe04a7f96e479195a47710abcf72be",
                  "preferred": true,
                  "validFor": {
                     "startDateTime": "2018-09-21T23:20:50.52Z"
                  },
                  "emailAddress": "neo@matrix.com"
               },
               "relationDate": "2018-09-21T23:20:50.52Z"
            },
            {
               "@type": "RelatedContactMedium",
               "role": "credential-login-alias-phone",
               "contactMedium": {
                  "@type": "PhoneContactMedium",
                  "@baseType": "ContactMedium",
                  "contactType": "private",
                  "id": "c0181f3d83e144a59162fd6136a98462",
                  "preferred": true,
                  "validFor": {
                     "startDateTime": "2018-09-21T23:20:50.52Z"
                  },
                  "phoneNumber": "+1 202-918-2132"
               },
               "relationDate": "2018-09-21T23:20:50.52Z"
            }
         ],
         "login": "neo1999",
         "creationDate": "2018-09-21T09:13:16-07:00",
         "lastUpdate": "2018-09-21T23:20:50.52Z"
      }
   ],
   "relatedContactMedium": [
      {
         "@type": "RelatedContactMedium",
         "role": "digital-id-recovery-email",
         "contactMedium": {
            "@type": "EmailContactMedium",
            "@baseType": "ContactMedium",
            "contactType": "private",
            "id": "b2fe04a7f96e479195a47710abcf72be",
```

```
            "preferred": true,
            "validFor": {
               "startDateTime": "2018-09-21T23:20:50.52Z"
            },
            "emailAddress": "neo@matrix.com"
         },
         "relationDate": "2018-09-21T23:20:50.52Z"
      },
      {
         "@type": "RelatedContactMedium",
         "role": "digital-id-recovery-phone",
         "contactMedium": {
            "@type": "PhoneContactMedium",
            "@baseType": "ContactMedium",
            "contactType": "private",
            "id": "60703a48038e4fc9a46bf1459aa3590f",
            "preferred": false,
            "validFor": {
               "startDateTime": "2018-09-21T23:20:50.52Z"
            },
            "phoneNumber": "+1 202-918-2132"
         },
         "relationDate": "2018-09-21T23:20:50.52Z"
      },
      {
         "@type": "RelatedContactMedium",
         "role": "digital-id-2nd-factor-phone",
         "contactMedium": {
            "@type": "PhoneContactMedium",
            "@baseType": "ContactMedium",
            "contactType": "private",
            "id": "c0181f3d83e144a59162fd6136a98462",
            "preferred": true,
            "validFor": {
               "startDateTime": "2018-09-21T23:20:50.52Z"
            },
            "phoneNumber": "+1 202-918-2132"
         },
         "relationDate": "2018-09-21T23:20:50.52Z"
      }
   ],
   "attachment": [
      {
         "@type": "Attachment",
         "attachmentType": "avatarPicture",
         "name": "Neo's avatar",
         "url": "https://i.pravatar.cc/150?u=neo",
         "mimeType": "image/jpeg",
         "size": {
            "amount": 91,
            "units": "Kb"
         },
         "validFor": {
            "startDateTime": "2018-09-21T23:20:50.52Z"
         }
      }
   ],
   "partyRoleIdentified": [
      {
         "@type": "RelatedSecurityPrincipalRef",
         "role": "Customer",
         "securityPrincipalRef": {
            "href": "https://serverRoot/tmf-
```

```
api/customerManagement/v5/partyRole/faa43dccaad142289e2b0f0e73e15958",
            "id": "faa43dccaad142289e2b0f0e73e15958",
            "@type": "PartyRoleRef",
            "@referredType": "PartyRole"
         }
      }
   ],
   "individualIdentified": {
      "href": "https://serverRoot/tmf-
api/partyManagement/v5/individual/193c8d6887394ca5b50290685db512ca",
      "id": "193c8d6887394ca5b50290685db512ca",
      "@type": "IndividualRef",
      "@referredType": "Individual"
   },
   "relatedSecurityPrincipal": [
      {
         "@type": "RelatedSecurityPrincipalRef",
         "role": "ServiceProvider",
         "securityPrincipalRef": {
            "href": "https://serverRoot/tmf-
api/partyManagement/v5/organization/e9b93f395a11453f9b7aa3349e857c24",
            "id": "e9b93f395a11453f9b7aa3349e857c24",
            "@type": "OrganizationRef",
            "@referredType": "Organization",
            "name": "Acme Inc."
         }
      },
      {
         "@type": "RelatedSecurityPrincipalRef",
         "role": "DigitalIdentityProvider",
         "securityPrincipalRef": {
            "href": "https://serverRoot/tmf-
api/partyManagement/v5/organization/af08cfda572749b0b4a90dfb75dfca51",
            "id": "af08cfda572749b0b4a90dfb75dfca51",
            "@type": "OrganizationRef",
            "@referredType": "Organization",
            "name": "Auth0"
         }
      }
   ],
   "creationDate": "2018-09-21T09:13:16-07:00",
   "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```


## Deletes a DigitalIdentity

**`DELETE /digitalIdentity/{id}`**

### Description

This operation deletes a DigitalIdentity entity.

### Usage samples

Example of a request to delete a specific digital identity.

### Request

```
DELETE /digitalIdentity/2391ee4acbc142b1a4b74b4d4ab38152
Content-Type: application/json
```

### Response

```
204
```

## Operations on CheckCredential

### Retrieves a CheckCredential by ID

**`GET /checkCredential/{id}?fields=…`**

#### Description

This operation retrieves a CheckCredential entity. Attribute selection is enabled for all first level attributes. Filtering may be available depending on the compliance level supported by an implementation.

#### Usage samples

Example of a request for retrieving a check login password credential task resource with a success result.

#### Request

```
GET /checkCredential/bf0fc07cff1946079548b7edb0d0db05
Content-Type: application/json
```

#### Response

```
200

{
   "id": "bf0fc07cff1946079548b7edb0d0db05",
   "@type": "CheckCredential",
   "credential": {
      "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/loginPasswordCredential/41af4b86e0b144cb9099b3d4c3a
b26ae",
      "id": "41af4b86e0b144cb9099b3d4c3ab26ae",
      "@type": "LoginPasswordCredential",
      "@baseType": "Credential",
      "state": "Active",
      "validFor": {
         "startDateTime": "2018-09-21T23:20:50.52Z"
      },
      "trustLevel": "high",
      "login": "neo1999",
      "digitalIdentity": {
         "href": "https://serverRoot/tmf-
```

```
api/digitalIdentityManagement/v5/digitalIdentity/2391ee4acbc142b1a4b74b4d4ab38152",
         "id": "2391ee4acbc142b1a4b74b4d4ab38152",
         "@type": "DigitalIdentityRef",
         "@referredType": "DigitalIdentity"
      },
      "creationDate": "2018-09-21T09:13:16-07:00",
      "lastUpdate": "2018-09-21T23:20:50.52Z"
   },
   "creationDate": "2018-09-21T09:13:16-07:00",
   "status": "succeded",
   "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```

Example of a request for retrieving a check login password credential task resource with a failed result.

### Request

```
GET /checkCredential/bf0fc07cff1946079548b7edb0d0db05
Content-Type: application/json
```

### Response

```
200

{
   "id": "bf0fc07cff1946079548b7edb0d0db05",
   "@type": "CheckCredential",
   "credential": {
      "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/loginPasswordCredential/41af4b86e0b144cb9099b3d4c3a
b26ae",
      "id": "41af4b86e0b144cb9099b3d4c3ab26ae",
      "@type": "LoginPasswordCredential",
      "@baseType": "Credential",
      "state": "Active",
      "validFor": {
         "startDateTime": "2018-09-21T23:20:50.52Z"
      },
      "trustLevel": "high",
      "login": "neo1999",
      "digitalIdentity": {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/digitalIdentity/2391ee4acbc142b1a4b74b4d4ab38152",
         "id": "2391ee4acbc142b1a4b74b4d4ab38152",
         "@type": "DigitalIdentityRef",
         "@referredType": "DigitalIdentity"
      },
      "creationDate": "2018-09-21T09:13:16-07:00",
      "lastUpdate": "2018-09-21T23:20:50.52Z"
   },
   "creationDate": "2018-09-21T09:13:16-07:00",
   "status": "failed",
   "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```

## List or find CheckCredential objects

`GET /checkCredential?fields=…`

### Description

This operation list CheckCredential entities. Attribute selection is enabled for all first level attributes. Filtering may be available depending on the compliance level supported by an implementation.

### Usage samples

Example of a request for retrieving a list of check credential task resources.

### Request

```
GET /checkCredential?state=succeded
Content-Type: application/json
```

### Response

```
200

[
   {
      "id": "bf0fc07cff1946079548b7edb0d0db05",
      "@type": "CheckCredential",
      "credential": {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/loginPasswordCredential/41af4b86e0b144cb9099b3d4c3a
b26ae",
         "id": "41af4b86e0b144cb9099b3d4c3ab26ae",
         "@type": "LoginPasswordCredential",
         "@baseType": "Credential",
         "state": "Active",
         "validFor": {
            "startDateTime": "2018-09-21T23:20:50.52Z"
         },
         "trustLevel": "high",
         "login": "neo1999",
         "digitalIdentity": {
            "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/digitalIdentity/2391ee4acbc142b1a4b74b4d4ab38152",
            "id": "2391ee4acbc142b1a4b74b4d4ab38152",
            "@type": "DigitalIdentityRef",
            "@referredType": "DigitalIdentity"
         },
         "creationDate": "2018-09-21T09:13:16-07:00",
         "lastUpdate": "2018-09-21T23:20:50.52Z"
      },
      "creationDate": "2018-09-21T09:13:16-07:00",
      "status": "succeded",
      "lastUpdate": "2018-09-21T23:20:50.52Z"
   }
]
```

## Creates a CheckCredential

**POST /checkCredential?fields=…**

### Description

This operation creates a CheckCredential entity.

### Mandatory Attributes

| Mandatory Attributes | Rule |
|---|---|
| credential | |
| credential.@type | |
| credential.id | |
| credential.login | |
| credential.state | |
| credential.trustLevel | |
| credential.validFor | |
| id | |
| @type | |

### Usage samples

Creation of a new check login password credential task resource with POST operation.

### Request

```
POST /checkCredential
Content-Type: application/json

{
   "@type": "CheckCredential",
   "credential": {
      "@type": "LoginPasswordCredential",
      "@baseType": "Credential",
      "login": "neo1999",
      "password": "*******"
   }
}
```

### Response

```
200

{
   "id": "bf0fc07cff1946079548b7edb0d0db05",
   "@type": "CheckCredential",
   "credential": {
      "href": "https://serverRoot/tmf-
```

```
api/digitalIdentityManagement/v5/loginPasswordCredential/41af4b86e0b144cb9099b3d4c3a
b26ae",
      "id": "41af4b86e0b144cb9099b3d4c3ab26ae",
      "@type": "LoginPasswordCredential",
      "@baseType": "Credential",
      "state": "Active",
      "validFor": {
         "startDateTime": "2018-09-21T23:20:50.52Z"
      },
      "trustLevel": "high",
      "login": "neo1999",
      "digitalIdentity": {
         "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/digitalIdentity/2391ee4acbc142b1a4b74b4d4ab38152",
         "id": "2391ee4acbc142b1a4b74b4d4ab38152",
         "@type": "DigitalIdentityRef",
         "@referredType": "DigitalIdentity"
      },
      "creationDate": "2018-09-21T09:13:16-07:00",
      "lastUpdate": "2018-09-21T23:20:50.52Z"
   },
   "creationDate": "2018-09-21T09:13:16-07:00",
   "status": "succeded",
   "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```


## Operations on Credential

### List or find Credential objects

**`GET /credential?fields=…`**

#### Description

This operation list Credential entities. Attribute selection is enabled for all first level attributes. Filtering may be available depending on the compliance level supported by an implementation.

#### Usage samples

Example of a request for retrieving a list of credentials (biometric, dongle, login password, network and token) in active state.

#### Request

```
GET /credential?state=Active
Content-Type: application/json
```

#### Response

```
200

[
   {
```

```
      "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/biometricCredential/754ea8ed4bef49d78ca2ba3f953cd65
f",
      "id": "754ea8ed4bef49d78ca2ba3f953cd65f",
      "@type": "BiometricCredential",
      "@baseType": "Credential",
      "state": "Active",
      "validFor": {
         "startDateTime": "2018-09-21T23:20:50.52Z"
      },
      "trustLevel": "high",
      "biometricType": "finger",
      "biometricSubType": "thumb",
      "attachment": [
         {
            "@type": "Attachment",
            "attachmentType": "thumbFingerprint",
            "name": "Thumb fingerprint",
            "content": "d2VyZndlcmZyd2VyZXJ3Zn...",
            "mimeType": "image/png",
            "size": {
               "amount": 104,
               "units": "Kb"
            },
            "validFor": {
               "startDateTime": "2018-09-21T23:20:50.52Z"
            }
         }
      ],
      "creationDate": "2018-09-21T09:13:16-07:00",
      "lastUpdate": "2018-09-21T23:20:50.52Z"
   },
   {
      "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/dongleCredential/f4435d1e425a420da6e80abb4c075b22",
      "id": "f4435d1e425a420da6e80abb4c075b22",
      "@type": "DongleCredential",
      "@baseType": "Credential",
      "state": "Active",
      "validFor": {
         "startDateTime": "2018-09-21T23:20:50.52Z"
      },
      "trustLevel": "high",
      "securityKeyId": "AE7671DF35BD581F467AB9B3DCF92",
      "securityKeyType": "USB Security Key",
      "securityKeyProvider": "Yubico",
      "creationDate": "2018-09-21T09:13:16-07:00",
      "lastUpdate": "2018-09-21T23:20:50.52Z"
   },
   {
      "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/loginPasswordCredential/41af4b86e0b144cb9099b3d4c3a
b26ae",
      "id": "41af4b86e0b144cb9099b3d4c3ab26ae",
      "@type": "LoginPasswordCredential",
      "@baseType": "Credential",
      "state": "Active",
      "validFor": {
         "startDateTime": "2018-09-21T23:20:50.52Z"
      },
      "trustLevel": "high",
      "relatedContactMedium": [
         {
```

```
            "@type": "RelatedContactMedium",
            "role": "credential-login-alias-email",
            "contactMedium": {
               "@type": "EmailContactMedium",
               "@baseType": "ContactMedium",
               "contactType": "private",
               "id": "b2fe04a7f96e479195a47710abcf72be",
               "preferred": true,
               "validFor": {
                  "startDateTime": "2018-09-21T23:20:50.52Z"
               },
               "emailAddress": "neo@matrix.com"
            },
            "relationDate": "2018-09-21T23:20:50.52Z"
         },
         {
            "@type": "RelatedContactMedium",
            "role": "credential-login-alias-phone",
            "contactMedium": {
               "@type": "PhoneContactMedium",
               "@baseType": "ContactMedium",
               "contactType": "private",
               "id": "c0181f3d83e144a59162fd6136a98462",
               "preferred": true,
               "validFor": {
                  "startDateTime": "2018-09-21T23:20:50.52Z"
               },
               "phoneNumber": "+1 202-918-2132"
            },
            "relationDate": "2018-09-21T23:20:50.52Z"
         }
      ],
      "login": "neo1999",
      "creationDate": "2018-09-21T09:13:16-07:00",
      "lastUpdate": "2018-09-21T23:20:50.52Z"
   },
   {
      "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/networkCredential/9fd97c82b4bf4fe7bcbee314d811290b"
,
      "id": "9fd97c82b4bf4fe7bcbee314d811290b",
      "@type": "NetworkCredential",
      "@baseType": "Credential",
      "state": "Active",
      "validFor": {
         "startDateTime": "2018-09-21T23:20:50.52Z"
      },
      "trustLevel": "high",
      "resource": {
         "@type": "ResourceRef",
         "id": "99729be76fa948d5a1df22618bec96ea"
      },
      "creationDate": "2018-09-21T09:13:16-07:00",
      "lastUpdate": "2018-09-21T23:20:50.52Z"
   },
   {
      "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/tokenCredential/7ef64b30fd5345ac9ab9554798c21f5c",
      "id": "7ef64b30fd5345ac9ab9554798c21f5c",
      "@type": "TokenCredential",
      "@baseType": "Credential",
      "state": "Active",
      "validFor": {
```

```
         "startDateTime": "2018-09-21T23:20:50.52Z",
         "endDateTime": "2018-10-21T23:20:50.52Z"
      },
      "trustLevel": "high",
      "login": "google.id:107691503500061507151130823 67",
      "tokenCredential":
"6nxugrzcv0e4se81kufqf0nn0rpygf4yqzyp7gha68wgqdpm057lx97jiiy6fdpq",
      "creationDate": "2018-09-21T09:13:16-07:00",
      "lastUpdate": "2018-09-21T23:20:50.52Z"
   }
]
```


## Retrieves a Credential by ID

**`GET /credential/{id}?fields=…`**

### Description

This operation retrieves a Credential entity. Attribute selection is enabled for all first level attributes. Filtering may be available depending on the compliance level supported by an implementation.

### Usage samples

Example of a request for retrieving a specific biometric credential with id 754ea8ed4bef49d78ca2ba3f953cd65f.

### Request

```
GET /credential/754ea8ed4bef49d78ca2ba3f953cd65f
Content-Type: application/json
```

### Response


```
200

{
   "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/biometricCredential/754ea8ed4bef49d78ca2ba3f953cd65
f",
   "id": "754ea8ed4bef49d78ca2ba3f953cd65f",
   "@type": "BiometricCredential",
   "@baseType": "Credential",
   "state": "Active",
   "validFor": {
      "startDateTime": "2018-09-21T23:20:50.52Z"
   },
   "trustLevel": "high",
   "biometricType": "finger",
   "biometricSubType": "thumb",
   "attachment": [
      {
         "@type": "Attachment",
         "attachmentType": "thumbFingerprint",
         "name": "Thumb fingerprint",
```

```
          "content": "d2VyZndlcmZyd2VyZXJ3Zn...",
          "mimeType": "image/png",
          "size": {
             "amount": 104,
             "units": "Kb"
          },
          "validFor": {
             "startDateTime": "2018-09-21T23:20:50.52Z"
          }
       }
    ],
    "creationDate": "2018-09-21T09:13:16-07:00",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```

Example of a request for retrieving a specific dongle credential with id f4435d1e425a420da6e80abb4c075b22.

**Request**

```
GET /credential/f4435d1e425a420da6e80abb4c075b22
Content-Type: application/json
```

**Response**

```
200

{
    "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/dongleCredential/f4435d1e425a420da6e80abb4c075b22",
    "id": "f4435d1e425a420da6e80abb4c075b22",
    "@type": "DongleCredential",
    "@baseType": "Credential",
    "state": "Active",
    "validFor": {
        "startDateTime": "2018-09-21T23:20:50.52Z"
    },
    "trustLevel": "high",
    "securityKeyId": "AE7671DF35BD581F467AB9B3DCF92",
    "securityKeyType": "USB Security Key",
    "securityKeyProvider": "Yubico",
    "creationDate": "2018-09-21T09:13:16-07:00",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```

Example of a request for retrieving a specific login password credential with id 41af4b86e0b144cb9099b3d4c3ab26ae.

**Request**

```
GET /credential/41af4b86e0b144cb9099b3d4c3ab26ae
Content-Type: application/json
```

### Response


```
200

{
    "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/loginPasswordCredential/41af4b86e0b144cb9099b3d4c3a
b26ae",
    "id": "41af4b86e0b144cb9099b3d4c3ab26ae",
    "@type": "LoginPasswordCredential",
    "@baseType": "Credential",
    "state": "Active",
    "validFor": {
        "startDateTime": "2018-09-21T23:20:50.52Z"
    },
    "trustLevel": "high",
    "relatedContactMedium": [
        {
            "@type": "RelatedContactMedium",
            "role": "credential-login-alias-email",
            "contactMedium": {
                "@type": "EmailContactMedium",
                "@baseType": "ContactMedium",
                "contactType": "private",
                "id": "b2fe04a7f96e479195a47710abcf72be",
                "preferred": true,
                "validFor": {
                    "startDateTime": "2018-09-21T23:20:50.52Z"
                },
                "emailAddress": "neo@matrix.com"
            },
            "relationDate": "2018-09-21T23:20:50.52Z"
        },
        {
            "@type": "RelatedContactMedium",
            "role": "credential-login-alias-phone",
            "contactMedium": {
                "@type": "PhoneContactMedium",
                "@baseType": "ContactMedium",
                "contactType": "private",
                "id": "c0181f3d83e144a59162fd6136a98462",
                "preferred": true,
                "validFor": {
                    "startDateTime": "2018-09-21T23:20:50.52Z"
                },
                "phoneNumber": "+1 202-918-2132"
            },
            "relationDate": "2018-09-21T23:20:50.52Z"
        }
    ],
    "login": "neo1999",
    "creationDate": "2018-09-21T09:13:16-07:00",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```


Example of a request for retrieving a specific network credential with id 9fd97c82b4bf4fe7bcbee314d811290b.

### Request

```
GET /credential/9fd97c82b4bf4fe7bcbee314d811290b
Content-Type: application/json
```

### Response

```
200

{
    "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/networkCredential/9fd97c82b4bf4fe7bcbee314d811290b"
,
    "id": "9fd97c82b4bf4fe7bcbee314d811290b",
    "@type": "NetworkCredential",
    "@baseType": "Credential",
    "state": "Active",
    "validFor": {
        "startDateTime": "2018-09-21T23:20:50.52Z"
    },
    "trustLevel": "high",
    "resource": {
        "@type": "ResourceRef",
        "id": "99729be76fa948d5a1df22618bec96ea"
    },
    "creationDate": "2018-09-21T09:13:16-07:00",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```

Example of a request for retrieving a specific token credential with id 7ef64b30fd5345ac9ab9554798c21f5c.

### Request

```
GET /credential/7ef64b30fd5345ac9ab9554798c21f5c
Content-Type: application/json
```

### Response

```
200

{
    "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/tokenCredential/7ef64b30fd5345ac9ab9554798c21f5c",
    "id": "7ef64b30fd5345ac9ab9554798c21f5c",
    "@type": "TokenCredential",
    "@baseType": "Credential",
    "state": "Active",
    "validFor": {
        "startDateTime": "2018-09-21T23:20:50.52Z",
        "endDateTime": "2018-10-21T23:20:50.52Z"
    },
    "trustLevel": "high",
    "login": "google.id:107691503500061507151130823 67",
    "tokenCredential":
"6nxugrzcv0e4se81kufqf0nn0rpygf4yqzyp7gha68wgqdpm057lx97jiiy6fdpq",
```

```
    "creationDate": "2018-09-21T09:13:16-07:00",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```

Example of a request for retrieving a specific biometric credential with id d1658f44a8d54b38b4f17eb6dcf73f92.

### Request

```
GET /credential/d1658f44a8d54b38b4f17eb6dcf73f92
Content-Type: application/json
```

### Response

```
200

{
   "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/tokenCredential/d1658f44a8d54b38b4f17eb6dcf73f92",
   "id": "d1658f44a8d54b38b4f17eb6dcf73f92",
   "@type": "TokenCredential",
   "@baseType": "Credential",
   "state": "Active",
   "validFor": {
      "startDateTime": "2018-09-21T23:20:50.52Z",
      "endDateTime": "2018-09-21T23:50:50.52Z"
   },
   "trustLevel": "high",
   "tokenCredential": "3452",
   "relatedContactMedium": [
      {
         "@type": "RelatedContactMedium",
         "role": "password-reset-phone-first-step",
         "contactMedium": {
            "@type": "PhoneContactMedium",
            "@baseType": "ContactMedium",
            "contactType": "private",
            "id": "60703a48038e4fc9a46bf1459aa3590f",
            "preferred": false,
            "validFor": {
               "startDateTime": "2018-09-21T23:20:50.52Z"
            },
            "phoneNumber": "+1 202-918-2132"
         },
         "relationDate": "2018-09-21T23:20:50.52Z"
      },
      {
         "@type": "RelatedContactMedium",
         "role": "password-reset-phone-confirmation-step",
         "contactMedium": {
            "@type": "PhoneContactMedium",
            "@baseType": "ContactMedium",
            "contactType": "private",
            "id": "60703a48038e4fc9a46bf1459aa3590f",
            "preferred": false,
            "validFor": {
               "startDateTime": "2018-09-21T23:20:50.52Z"
```

```
            },
            "phoneNumber": "+1 202-918-2132"
         },
         "relationDate": "2018-09-21T23:20:50.52Z"
      }
   ],
   "creationDate": "2018-09-21T09:13:16-07:00",
   "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```


## Creates a Credential

### POST /credential?fields=…

#### Description

This operation creates a Credential entity.

#### Mandatory Attributes

| Mandatory Attributes | Rule |
|---|---|
| id | |
| state | |
| trustLevel | |
| validFor | |
| @type | |

#### Usage samples

Creation of a new biometric credential with POST operation.

#### Request


```
POST /credential
Content-Type: application/json

{
    "@type": "BiometricCredential",
    "@baseType": "Credential",
    "biometricType": "finger",
    "biometricSubType": "thumb",
    "attachment": [
       {
          "@type": "Attachment",
          "attachmentType": "thumbFingerprint",
          "name": "Thumb fingerprint",
          "content": "d2VyZndlcmZyd2VyZXJ3Zn...",
          "mimeType": "image/png",
          "size": {
             "amount": 104,
             "units": "Kb"
          },
          "validFor": {
```

```
            "startDateTime": "2018-09-21T23:20:50.52Z"
         }
      }
   ]
}
```

### Response

```
201

{
    "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/biometricCredential/754ea8ed4bef49d78ca2ba3f953cd65
f",
    "id": "754ea8ed4bef49d78ca2ba3f953cd65f",
    "@type": "BiometricCredential",
    "@baseType": "Credential",
    "state": "Active",
    "validFor": {
       "startDateTime": "2018-09-21T23:20:50.52Z"
    },
    "trustLevel": "high",
    "biometricType": "finger",
    "biometricSubType": "thumb",
    "attachment": [
       {
          "@type": "Attachment",
          "attachmentType": "thumbFingerprint",
          "name": "Thumb fingerprint",
          "content": "d2VyZndlcmZyd2VyZXJ3Zn...",
          "mimeType": "image/png",
          "size": {
             "amount": 104,
             "units": "Kb"
          },
          "validFor": {
             "startDateTime": "2018-09-21T23:20:50.52Z"
          }
       }
    ],
    "creationDate": "2018-09-21T09:13:16-07:00",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```

Creation of a new dongle credential with POST operation.

### Request

```
POST /credential
Content-Type: application/json

{
    "@type": "DongleCredential",
    "@baseType": "Credential",
    "securityKeyId": "AE7671DF35BD581F467AB9B3DCF92",
    "securityKeyType": "USB Security Key",
    "securityKeyProvider": "Yubico"
```

```
}
```

### Response

```
201

{
    "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/dongleCredential/f4435d1e425a420da6e80abb4c075b22",
    "id": "f4435d1e425a420da6e80abb4c075b22",
    "@type": "DongleCredential",
    "@baseType": "Credential",
    "state": "Active",
    "validFor": {
        "startDateTime": "2018-09-21T23:20:50.52Z"
    },
    "trustLevel": "high",
    "securityKeyId": "AE7671DF35BD581F467AB9B3DCF92",
    "securityKeyType": "USB Security Key",
    "securityKeyProvider": "Yubico",
    "creationDate": "2018-09-21T09:13:16-07:00",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```

Creation of a new login password credential with POST operation.

### Request

```
POST /credential
Content-Type: application/json

{
    "@type": "LoginPasswordCredential",
    "@baseType": "Credential",
    "relatedContactMedium": [
       {
          "@type": "RelatedContactMedium",
          "role": "credential-login-alias-email",
          "contactMedium": {
             "@type": "EmailContactMedium",
             "@baseType": "ContactMedium",
             "contactType": "private",
             "id": "b2fe04a7f96e479195a47710abcf72be",
             "preferred": true,
             "validFor": {
                "startDateTime": "2018-09-21T23:20:50.52Z"
             },
             "emailAddress": "neo@matrix.com"
          },
          "relationDate": "2018-09-21T23:20:50.52Z"
       },
       {
          "@type": "RelatedContactMedium",
          "role": "credential-login-alias-phone",
          "contactMedium": {
             "@type": "PhoneContactMedium",
             "@baseType": "ContactMedium",
```

```
            "contactType": "private",
            "id": "c0181f3d83e144a59162fd6136a98462",
            "preferred": true,
            "validFor": {
               "startDateTime": "2018-09-21T23:20:50.52Z"
            },
            "phoneNumber": "+1 202-918-2132"
         },
         "relationDate": "2018-09-21T23:20:50.52Z"
      }
   ],
   "login": "neo1999",
   "password": "*******"
}
```


### Response


```
201

{
    "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/loginPasswordCredential/41af4b86e0b144cb9099b3d4c3a
b26ae",
    "id": "41af4b86e0b144cb9099b3d4c3ab26ae",
    "@type": "LoginPasswordCredential",
    "@baseType": "Credential",
    "state": "Active",
    "validFor": {
       "startDateTime": "2018-09-21T23:20:50.52Z"
    },
    "trustLevel": "high",
    "relatedContactMedium": [
       {
          "@type": "RelatedContactMedium",
          "role": "credential-login-alias-email",
          "contactMedium": {
             "@type": "EmailContactMedium",
             "@baseType": "ContactMedium",
             "contactType": "private",
             "id": "b2fe04a7f96e479195a47710abcf72be",
             "preferred": true,
             "validFor": {
                "startDateTime": "2018-09-21T23:20:50.52Z"
             },
             "emailAddress": "neo@matrix.com"
          },
          "relationDate": "2018-09-21T23:20:50.52Z"
       },
       {
          "@type": "RelatedContactMedium",
          "role": "credential-login-alias-phone",
          "contactMedium": {
             "@type": "PhoneContactMedium",
             "@baseType": "ContactMedium",
             "contactType": "private",
             "id": "c0181f3d83e144a59162fd6136a98462",
             "preferred": true,
             "validFor": {
                "startDateTime": "2018-09-21T23:20:50.52Z"
             },
```

```
            "phoneNumber": "+1 202-918-2132"
          },
          "relationDate": "2018-09-21T23:20:50.52Z"
       }
    ],
    "login": "neo1999",
    "creationDate": "2018-09-21T09:13:16-07:00",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
 }
```

Creation of a new network credential with POST operation.

### Request

```
POST /credential
Content-Type: application/json

{
    "@type": "NetworkCredential",
    "@baseType": "Credential",
    "resource": {
        "@type": "ResourceRef",
        "id": "99729be76fa948d5a1df22618bec96ea"
    }
}
```

### Response

```
201

{
    "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/networkCredential/9fd97c82b4bf4fe7bcbee314d811290b"
,
    "id": "9fd97c82b4bf4fe7bcbee314d811290b",
    "@type": "NetworkCredential",
    "@baseType": "Credential",
    "state": "Active",
    "validFor": {
        "startDateTime": "2018-09-21T23:20:50.52Z"
    },
    "trustLevel": "high",
    "resource": {
        "@type": "ResourceRef",
        "id": "99729be76fa948d5a1df22618bec96ea"
    },
    "creationDate": "2018-09-21T09:13:16-07:00",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```

Creation of a new token credential with POST operation (federated identity token).

### Request

```
POST /credential
```

```
Content-Type: application/json

{
    "@type": "TokenCredential",
    "@baseType": "Credential",
    "login": "google.id:107691503500061507151130823 67",
    "tokenCredential":
"6nxugrzcv0e4se81kufqf0nn0rpygf4yqzyp7gha68wgqdpm057lx97jiiy6fdpq"
}
```

### Response

```
201

{
    "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/tokenCredential/7ef64b30fd5345ac9ab9554798c21f5c",
    "id": "7ef64b30fd5345ac9ab9554798c21f5c",
    "@type": "TokenCredential",
    "@baseType": "Credential",
    "state": "Active",
    "validFor": {
        "startDateTime": "2018-09-21T23:20:50.52Z",
        "endDateTime": "2018-10-21T23:20:50.52Z"
    },
    "trustLevel": "high",
    "login": "google.id:107691503500061507151130823 67",
    "tokenCredential":
"6nxugrzcv0e4se81kufqf0nn0rpygf4yqzyp7gha68wgqdpm057lx97jiiy6fdpq",
    "creationDate": "2018-09-21T09:13:16-07:00",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```

Creation of a new token credential with POST operation (password reset token).

### Request

```
POST /credential
Content-Type: application/json

{
    "@type": "TokenCredential",
    "@baseType": "Credential",
    "tokenCredential": "3452",
    "relatedContactMedium": [
       {
          "@type": "RelatedContactMedium",
          "role": "password-reset-phone-first-step",
          "contactMedium": {
             "@type": "PhoneContactMedium",
             "@baseType": "ContactMedium",
             "contactType": "private",
             "id": "60703a48038e4fc9a46bf1459aa3590f",
             "preferred": false,
             "validFor": {
                "startDateTime": "2018-09-21T23:20:50.52Z"
             },
```

```
            "phoneNumber": "+1 202-918-2132"
         },
         "relationDate": "2018-09-21T23:20:50.52Z"
      },
      {
         "@type": "RelatedContactMedium",
         "role": "password-reset-phone-confirmation-step",
         "contactMedium": {
            "@type": "PhoneContactMedium",
            "@baseType": "ContactMedium",
            "contactType": "private",
            "id": "60703a48038e4fc9a46bf1459aa3590f",
            "preferred": false,
            "validFor": {
               "startDateTime": "2018-09-21T23:20:50.52Z"
            },
            "phoneNumber": "+1 202-918-2132"
         },
         "relationDate": "2018-09-21T23:20:50.52Z"
      }
   ]
}
```


## Response


```
201

{
    "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/tokenCredential/d1658f44a8d54b38b4f17eb6dcf73f92",
    "id": "d1658f44a8d54b38b4f17eb6dcf73f92",
    "@type": "TokenCredential",
    "@baseType": "Credential",
    "state": "Active",
    "validFor": {
       "startDateTime": "2018-09-21T23:20:50.52Z",
       "endDateTime": "2018-09-21T23:50:50.52Z"
    },
    "trustLevel": "high",
    "tokenCredential": "3452",
    "relatedContactMedium": [
       {
          "@type": "RelatedContactMedium",
          "role": "password-reset-phone-first-step",
          "contactMedium": {
             "@type": "PhoneContactMedium",
             "@baseType": "ContactMedium",
             "contactType": "private",
             "id": "60703a48038e4fc9a46bf1459aa3590f",
             "preferred": false,
             "validFor": {
                "startDateTime": "2018-09-21T23:20:50.52Z"
             },
             "phoneNumber": "+1 202-918-2132"
          },
          "relationDate": "2018-09-21T23:20:50.52Z"
       },
       {
          "@type": "RelatedContactMedium",
          "role": "password-reset-phone-confirmation-step",
```

```
            "contactMedium": {
               "@type": "PhoneContactMedium",
               "@baseType": "ContactMedium",
               "contactType": "private",
               "id": "60703a48038e4fc9a46bf1459aa3590f",
               "preferred": false,
               "validFor": {
                  "startDateTime": "2018-09-21T23:20:50.52Z"
               },
               "phoneNumber": "+1 202-918-2132"
            },
            "relationDate": "2018-09-21T23:20:50.52Z"
         }
      ],
      "creationDate": "2018-09-21T09:13:16-07:00",
      "lastUpdate": "2018-09-21T23:20:50.52Z"
   }
```


## Updates partially a Credential

**`PATCH /credential/{id}?fields=…`**

### Description

This operation allows partial updates of a Credential entity. Support of json/merge (https://tools.ietf.org/html/rfc7396) is mandatory, support of json/patch (http://tools.ietf.org/html/rfc5789) is optional. Note: If the update operation yields to the creation of sub-resources or relationships, the same rules concerning mandatory sub-resource attributes and default value settings in the POST operation applies to the PATCH operation. Hence these tables are not repeated here.

### Patchable and Non Patchable Attributes

| Non Patchable Attributes | Rule |
|---|---|
| creationDate | |
| href | |
| id | |
| state | |
| trustLevel | |
| validFor | |
| @baseType | @baseType is immutable |
| @schemaLocation | @schemaLocation is immutable |
| @type | @type is immutable |

| Patchable Attributes | Rule |
|---|---|
| digitalIdentity | |
| lastUpdate | |
| relatedContactMedium | |

### Usage samples

Example of a request for fully updating an entire biometric credential.

### Request

```
PATCH /credential/754ea8ed4bef49d78ca2ba3f953cd65f
Content-Type: application/json

{
   "@type": "BiometricCredential",
   "biometricType": "finger",
   "biometricSubType": "thumb",
   "attachment": [
      {
         "@type": "Attachment",
         "attachmentType": "thumbFingerprint",
         "name": "Thumb fingerprint",
         "content": "d2VyZndlcmZyd2VyZXJ3Zn...",
         "mimeType": "image/png",
         "size": {
            "amount": 104,
            "units": "Kb"
         },
         "validFor": {
            "startDateTime": "2018-09-21T23:20:50.52Z"
         }
      }
   ]
}
```

### Response

```
200

{
   "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/biometricCredential/754ea8ed4bef49d78ca2ba3f953cd65
f",
   "id": "754ea8ed4bef49d78ca2ba3f953cd65f",
   "@type": "BiometricCredential",
   "@baseType": "Credential",
   "state": "Active",
   "validFor": {
      "startDateTime": "2018-09-21T23:20:50.52Z"
   },
   "trustLevel": "high",
   "biometricType": "finger",
   "biometricSubType": "thumb",
   "attachment": [
      {
         "@type": "Attachment",
         "attachmentType": "thumbFingerprint",
         "name": "Thumb fingerprint",
         "content": "d2VyZndlcmZyd2VyZXJ3Zn...",
         "mimeType": "image/png",
         "size": {
            "amount": 104,
```

```
            "units": "Kb"
         },
         "validFor": {
            "startDateTime": "2018-09-21T23:20:50.52Z"
         }
      }
   ],
   "creationDate": "2018-09-21T09:13:16-07:00",
   "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```

Example of a request for partial updating a biometric credential, using MERGE Patch.

### Request

```
PATCH /credential/754ea8ed4bef49d78ca2ba3f953cd65f
Content-Type: application/merge-patch+json

{
   "@type": "BiometricCredential",
   "biometricType": "finger",
   "biometricSubType": "thumb",
   "attachment": [
      {
         "@type": "Attachment",
         "attachmentType": "thumbFingerprint",
         "name": "Thumb fingerprint",
         "content": "d2VyZndlcmZyd2VyZXJ3Zn...",
         "mimeType": "image/png",
         "size": {
            "amount": 104,
            "units": "Kb"
         },
         "validFor": {
            "startDateTime": "2018-09-21T23:20:50.52Z"
         }
      }
   ]
}
```

### Response

```
200

{
   "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/biometricCredential/754ea8ed4bef49d78ca2ba3f953cd65
f",
   "id": "754ea8ed4bef49d78ca2ba3f953cd65f",
   "@type": "BiometricCredential",
   "@baseType": "Credential",
   "state": "Active",
   "validFor": {
      "startDateTime": "2018-09-21T23:20:50.52Z"
   },
   "trustLevel": "high",
   "biometricType": "finger",
```

```
    "biometricSubType": "thumb",
    "attachment": [
       {
          "@type": "Attachment",
          "attachmentType": "thumbFingerprint",
          "name": "Thumb fingerprint",
          "content": "d2VyZndlcmZyd2VyZXJ3Zn...",
          "mimeType": "image/png",
          "size": {
             "amount": 104,
             "units": "Kb"
          },
          "validFor": {
             "startDateTime": "2018-09-21T23:20:50.52Z"
          }
       }
    ],
    "creationDate": "2018-09-21T09:13:16-07:00",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```


Example of a request for partial updating a biometric credential, using JSON Patch.

**Request**


```
PATCH /credential/754ea8ed4bef49d78ca2ba3f953cd65f
Content-Type: application/json-patch+json

[
  {
    "op": "replace",
    "path": "/biometricType",
    "value": "finger"
  },
  {
    "op": "replace",
    "path": "/biometricSubType",
    "value": "thumb"
  },
  {
    "op": "replace",
    "path": "/attachment",
    "value": [
      {
        "@type": "Attachment",
        "attachmentType": "thumbFingerprint",
        "name": "Thumb fingerprint",
        "content": "d2VyZndlcmZyd2VyZXJ3Zn...",
        "mimeType": "image/png",
        "size": {
          "amount": 104,
          "units": "Kb"
        },
        "validFor": {
          "startDateTime": "2018-09-21T23:20:50.52Z"
        }
      }
    ]
  }
```

```
]
```

### Response

```
200

{
   "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/biometricCredential/754ea8ed4bef49d78ca2ba3f953cd65
f",
   "id": "754ea8ed4bef49d78ca2ba3f953cd65f",
   "@type": "BiometricCredential",
   "@baseType": "Credential",
   "state": "Active",
   "validFor": {
      "startDateTime": "2018-09-21T23:20:50.52Z"
   },
   "trustLevel": "high",
   "biometricType": "finger",
   "biometricSubType": "thumb",
   "attachment": [
      {
         "@type": "Attachment",
         "attachmentType": "thumbFingerprint",
         "name": "Thumb fingerprint",
         "content": "d2VyZndlcmZyd2VyZXJ3Zn...",
         "mimeType": "image/png",
         "size": {
            "amount": 104,
            "units": "Kb"
         },
         "validFor": {
            "startDateTime": "2018-09-21T23:20:50.52Z"
         }
      }
   ],
   "creationDate": "2018-09-21T09:13:16-07:00",
   "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```

Example of a request for partial updating a biometric credential, using JSON Patch Query.

### Request

```
PATCH /credential/754ea8ed4bef49d78ca2ba3f953cd65f
Content-Type: application/json-patch-query+json

[
  {
    "op": "remove",
    "path":
"/relatedContactMedium?contactMedium.id=116aca1739db4a57a9fbaebd0210b996"
  }
]
```

### Response

```
200

{
   "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/biometricCredential/754ea8ed4bef49d78ca2ba3f953cd65
f",
   "id": "754ea8ed4bef49d78ca2ba3f953cd65f",
   "@type": "BiometricCredential",
   "@baseType": "Credential",
   "state": "Active",
   "validFor": {
      "startDateTime": "2018-09-21T23:20:50.52Z"
   },
   "trustLevel": "high",
   "biometricType": "finger",
   "biometricSubType": "thumb",
   "attachment": [
      {
         "@type": "Attachment",
         "attachmentType": "thumbFingerprint",
         "name": "Thumb fingerprint",
         "content": "d2VyZndlcmZyd2VyZXJ3Zn...",
         "mimeType": "image/png",
         "size": {
            "amount": 104,
            "units": "Kb"
         },
         "validFor": {
            "startDateTime": "2018-09-21T23:20:50.52Z"
         }
      }
   ],
   "creationDate": "2018-09-21T09:13:16-07:00",
   "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```

Example of a request for fully updating an entire dongle credential.

### Request

```
PATCH /credential/f4435d1e425a420da6e80abb4c075b22
Content-Type: application/json

{
   "@type": "DongleCredential",
   "securityKeyId": "AE7671DF35BD581F467AB9B3DCF92",
   "securityKeyType": "USB Security Key",
   "securityKeyProvider": "Yubico"
}
```

### Response

```
200

{
    "href": "https://serverRoot/tmf-
```

```
api/digitalIdentityManagement/v5/dongleCredential/f4435d1e425a420da6e80abb4c075b22",
    "id": "f4435d1e425a420da6e80abb4c075b22",
    "@type": "DongleCredential",
    "@baseType": "Credential",
    "state": "Active",
    "validFor": {
        "startDateTime": "2018-09-21T23:20:50.52Z"
    },
    "trustLevel": "high",
    "securityKeyId": "AE7671DF35BD581F467AB9B3DCF92",
    "securityKeyType": "USB Security Key",
    "securityKeyProvider": "Yubico",
    "creationDate": "2018-09-21T09:13:16-07:00",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```


Example of a request for partial updating a dongle credential, using MERGE Patch.

### Request

```
PATCH /credential/f4435d1e425a420da6e80abb4c075b22
Content-Type: application/merge-patch+json

{
   "@type": "DongleCredential",
   "securityKeyId": "AE7671DF35BD581F467AB9B3DCF92",
   "securityKeyType": "USB Security Key",
   "securityKeyProvider": "Yubico"
}
```

### Response


```
200

{
    "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/dongleCredential/f4435d1e425a420da6e80abb4c075b22",
    "id": "f4435d1e425a420da6e80abb4c075b22",
    "@type": "DongleCredential",
    "@baseType": "Credential",
    "state": "Active",
    "validFor": {
        "startDateTime": "2018-09-21T23:20:50.52Z"
    },
    "trustLevel": "high",
    "securityKeyId": "AE7671DF35BD581F467AB9B3DCF92",
    "securityKeyType": "USB Security Key",
    "securityKeyProvider": "Yubico",
    "creationDate": "2018-09-21T09:13:16-07:00",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```


Example of a request for partial updating a dongle credential, using JSON Patch.

### Request

```
PATCH /credential/f4435d1e425a420da6e80abb4c075b22
Content-Type: application/json-patch+json

[
  {
    "op": "replace",
    "path": "/securityKeyId",
    "value": "AE7671DF35BD581F467AB9B3DCF92"
  },
  {
    "op": "replace",
    "path": "/securityKeyType",
    "value": "USB Security Key"
  },
  {
    "op": "replace",
    "path": "/securityKeyProvider",
    "value": "Yubico"
  }
]
```

### Response

```
200

{
    "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/dongleCredential/f4435d1e425a420da6e80abb4c075b22",
    "id": "f4435d1e425a420da6e80abb4c075b22",
    "@type": "DongleCredential",
    "@baseType": "Credential",
    "state": "Active",
    "validFor": {
        "startDateTime": "2018-09-21T23:20:50.52Z"
    },
    "trustLevel": "high",
    "securityKeyId": "AE7671DF35BD581F467AB9B3DCF92",
    "securityKeyType": "USB Security Key",
    "securityKeyProvider": "Yubico",
    "creationDate": "2018-09-21T09:13:16-07:00",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```

Example of a request for partial updating a dongle credential, using JSON Patch Query.

### Request

```
PATCH /credential/f4435d1e425a420da6e80abb4c075b22
Content-Type: application/json-patch-query+json

[
  {
    "op": "remove",
    "path":
"/relatedContactMedium?contactMedium.id=116aca1739db4a57a9fbaebd0210b996"
  }
```

```
]
```

### Response

```
200

{
    "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/dongleCredential/f4435d1e425a420da6e80abb4c075b22",
    "id": "f4435d1e425a420da6e80abb4c075b22",
    "@type": "DongleCredential",
    "@baseType": "Credential",
    "state": "Active",
    "validFor": {
        "startDateTime": "2018-09-21T23:20:50.52Z"
    },
    "trustLevel": "high",
    "securityKeyId": "AE7671DF35BD581F467AB9B3DCF92",
    "securityKeyType": "USB Security Key",
    "securityKeyProvider": "Yubico",
    "creationDate": "2018-09-21T09:13:16-07:00",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```

Example of a request for fully updating an entire login password credential.

### Request

```
PATCH /credential/41af4b86e0b144cb9099b3d4c3ab26ae
Content-Type: application/json

{
   "@type": "LoginPasswordCredential",
   "login": "neo1999",
   "password": "********"
}
```

### Response

```
200

{
   "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/loginPasswordCredential/41af4b86e0b144cb9099b3d4c3a
b26ae",
   "id": "41af4b86e0b144cb9099b3d4c3ab26ae",
   "@type": "LoginPasswordCredential",
   "@baseType": "Credential",
   "state": "Active",
   "validFor": {
      "startDateTime": "2018-09-21T23:20:50.52Z"
   },
   "trustLevel": "high",
   "relatedContactMedium": [
      {
```

```
         "@type": "RelatedContactMedium",
         "role": "credential-login-alias-email",
         "contactMedium": {
            "@type": "EmailContactMedium",
            "@baseType": "ContactMedium",
            "contactType": "private",
            "id": "b2fe04a7f96e479195a47710abcf72be",
            "preferred": true,
            "validFor": {
               "startDateTime": "2018-09-21T23:20:50.52Z"
            },
            "emailAddress": "neo@matrix.com"
         },
         "relationDate": "2018-09-21T23:20:50.52Z"
      },
      {
         "@type": "RelatedContactMedium",
         "role": "credential-login-alias-phone",
         "contactMedium": {
            "@type": "PhoneContactMedium",
            "@baseType": "ContactMedium",
            "contactType": "private",
            "id": "c0181f3d83e144a59162fd6136a98462",
            "preferred": true,
            "validFor": {
               "startDateTime": "2018-09-21T23:20:50.52Z"
            },
            "phoneNumber": "+1 202-918-2132"
         },
         "relationDate": "2018-09-21T23:20:50.52Z"
      }
   ],
   "login": "neo1999",
   "creationDate": "2018-09-21T09:13:16-07:00",
   "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```


Example of a request for partial updating a login password credential, using MERGE Patch.

### Request

```
PATCH /credential/41af4b86e0b144cb9099b3d4c3ab26ae
Content-Type: application/merge-patch+json

{
   "@type": "LoginPasswordCredential",
   "login": "neo1999",
   "password": "********"
}
```

### Response

```
200

{
   "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/loginPasswordCredential/41af4b86e0b144cb9099b3d4c3a
```

```
b26ae",
   "id": "41af4b86e0b144cb9099b3d4c3ab26ae",
   "@type": "LoginPasswordCredential",
   "@baseType": "Credential",
   "state": "Active",
   "validFor": {
      "startDateTime": "2018-09-21T23:20:50.52Z"
   },
   "trustLevel": "high",
   "relatedContactMedium": [
      {
         "@type": "RelatedContactMedium",
         "role": "credential-login-alias-email",
         "contactMedium": {
            "@type": "EmailContactMedium",
            "@baseType": "ContactMedium",
            "contactType": "private",
            "id": "b2fe04a7f96e479195a47710abcf72be",
            "preferred": true,
            "validFor": {
               "startDateTime": "2018-09-21T23:20:50.52Z"
            },
            "emailAddress": "neo@matrix.com"
         },
         "relationDate": "2018-09-21T23:20:50.52Z"
      },
      {
         "@type": "RelatedContactMedium",
         "role": "credential-login-alias-phone",
         "contactMedium": {
            "@type": "PhoneContactMedium",
            "@baseType": "ContactMedium",
            "contactType": "private",
            "id": "c0181f3d83e144a59162fd6136a98462",
            "preferred": true,
            "validFor": {
               "startDateTime": "2018-09-21T23:20:50.52Z"
            },
            "phoneNumber": "+1 202-918-2132"
         },
         "relationDate": "2018-09-21T23:20:50.52Z"
      }
   ],
   "login": "neo1999",
   "creationDate": "2018-09-21T09:13:16-07:00",
   "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```


Example of a request for partial updating a login password, using JSON Patch.

### Request

```
PATCH /credential/41af4b86e0b144cb9099b3d4c3ab26ae
Content-Type: application/json-patch+json

[
  {
    "op": "replace",
    "path": "/state",
    "value": "active"
```

```
  },
  {
    "op": "replace",
    "path": "/login",
    "value": "neo1999"
  },
  {
    "op": "replace",
    "path": "/password",
    "value": "**********"
  }
]
```

### Response

```
200

{
   "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/loginPasswordCredential/41af4b86e0b144cb9099b3d4c3a
b26ae",
   "id": "41af4b86e0b144cb9099b3d4c3ab26ae",
   "@type": "LoginPasswordCredential",
   "@baseType": "Credential",
   "state": "Active",
   "validFor": {
      "startDateTime": "2018-09-21T23:20:50.52Z"
   },
   "trustLevel": "high",
   "relatedContactMedium": [
      {
         "@type": "RelatedContactMedium",
         "role": "credential-login-alias-email",
         "contactMedium": {
            "@type": "EmailContactMedium",
            "@baseType": "ContactMedium",
            "contactType": "private",
            "id": "b2fe04a7f96e479195a47710abcf72be",
            "preferred": true,
            "validFor": {
               "startDateTime": "2018-09-21T23:20:50.52Z"
            },
            "emailAddress": "neo@matrix.com"
         },
         "relationDate": "2018-09-21T23:20:50.52Z"
      },
      {
         "@type": "RelatedContactMedium",
         "role": "credential-login-alias-phone",
         "contactMedium": {
            "@type": "PhoneContactMedium",
            "@baseType": "ContactMedium",
            "contactType": "private",
            "id": "c0181f3d83e144a59162fd6136a98462",
            "preferred": true,
            "validFor": {
               "startDateTime": "2018-09-21T23:20:50.52Z"
            },
            "phoneNumber": "+1 202-918-2132"
         },
```

```
          "relationDate": "2018-09-21T23:20:50.52Z"
       }
    ],
    "login": "neo1999",
    "creationDate": "2018-09-21T09:13:16-07:00",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```

Example of a request for partial updating a login password credential, using JSON Patch Query.

### Request

```
PATCH /credential/41af4b86e0b144cb9099b3d4c3ab26ae
Content-Type: application/json-patch-query+json

[
  {
    "op": "remove",
    "path":
"/relatedContactMedium?contactMedium.id=116aca1739db4a57a9fbaebd0210b996"
  }
]
```

### Response

```
200

{
    "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/loginPasswordCredential/41af4b86e0b144cb9099b3d4c3a
b26ae",
    "id": "41af4b86e0b144cb9099b3d4c3ab26ae",
    "@type": "LoginPasswordCredential",
    "@baseType": "Credential",
    "state": "Active",
    "validFor": {
       "startDateTime": "2018-09-21T23:20:50.52Z"
    },
    "trustLevel": "high",
    "relatedContactMedium": [
       {
          "@type": "RelatedContactMedium",
          "role": "credential-login-alias-email",
          "contactMedium": {
             "@type": "EmailContactMedium",
             "@baseType": "ContactMedium",
             "contactType": "private",
             "id": "b2fe04a7f96e479195a47710abcf72be",
             "preferred": true,
             "validFor": {
                "startDateTime": "2018-09-21T23:20:50.52Z"
             },
             "emailAddress": "neo@matrix.com"
          },
          "relationDate": "2018-09-21T23:20:50.52Z"
       },
```

```
        {
           "@type": "RelatedContactMedium",
           "role": "credential-login-alias-phone",
           "contactMedium": {
              "@type": "PhoneContactMedium",
              "@baseType": "ContactMedium",
              "contactType": "private",
              "id": "c0181f3d83e144a59162fd6136a98462",
              "preferred": true,
              "validFor": {
                 "startDateTime": "2018-09-21T23:20:50.52Z"
              },
              "phoneNumber": "+1 202-918-2132"
           },
           "relationDate": "2018-09-21T23:20:50.52Z"
        }
     ],
     "login": "neo1999",
     "creationDate": "2018-09-21T09:13:16-07:00",
     "lastUpdate": "2018-09-21T23:20:50.52Z"
  }
```

Example of a request for fully updating an entire network credential.

### Request

```
PATCH /credential/9fd97c82b4bf4fe7bcbee314d811290b
Content-Type: application/json

{
    "@type": "NetworkCredential",
    "password": "********",
    "resource": {
        "@type": "ResourceRef",
        "id": "99729be76fa948d5a1df22618bec96ea"
    }
}
```

### Response

```
200

{
    "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/networkCredential/9fd97c82b4bf4fe7bcbee314d811290b"
,
    "id": "9fd97c82b4bf4fe7bcbee314d811290b",
    "@type": "NetworkCredential",
    "@baseType": "Credential",
    "state": "Active",
    "validFor": {
        "startDateTime": "2018-09-21T23:20:50.52Z"
    },
    "trustLevel": "high",
    "resource": {
        "@type": "ResourceRef",
        "id": "99729be76fa948d5a1df22618bec96ea"
```

```
    },
    "creationDate": "2018-09-21T09:13:16-07:00",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```

Example of a request for partial updating a network credential, using MERGE Patch.

### Request

```
PATCH /credential/9fd97c82b4bf4fe7bcbee314d811290b
Content-Type: application/merge-patch+json

{
    "@type": "NetworkCredential",
    "password": "********",
    "resource": {
        "@type": "ResourceRef",
        "id": "99729be76fa948d5a1df22618bec96ea"
    }
}
```

### Response

```
200

{
    "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/networkCredential/9fd97c82b4bf4fe7bcbee314d811290b"
,
    "id": "9fd97c82b4bf4fe7bcbee314d811290b",
    "@type": "NetworkCredential",
    "@baseType": "Credential",
    "state": "Active",
    "validFor": {
        "startDateTime": "2018-09-21T23:20:50.52Z"
    },
    "trustLevel": "high",
    "resource": {
        "@type": "ResourceRef",
        "id": "99729be76fa948d5a1df22618bec96ea"
    },
    "creationDate": "2018-09-21T09:13:16-07:00",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```

Example of a request for partial updating a network credential, using JSON Patch.

### Request

```
PATCH /credential/9fd97c82b4bf4fe7bcbee314d811290b
Content-Type: application/json-patch+json

[
  {
    "op": "replace",
```

```
    "path": "/password",
    "value": "***"
  },
  {
    "op": "replace",
    "path": "/resource",
    "value": {
      "@type": "ResourceRef",
      "id": "99729be76fa948d5a1df22618bec96ea"
    }
  }
]
```

### Response

```
200

{
    "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/networkCredential/9fd97c82b4bf4fe7bcbee314d811290b"
,
    "id": "9fd97c82b4bf4fe7bcbee314d811290b",
    "@type": "NetworkCredential",
    "@baseType": "Credential",
    "state": "Active",
    "validFor": {
        "startDateTime": "2018-09-21T23:20:50.52Z"
    },
    "trustLevel": "high",
    "resource": {
        "@type": "ResourceRef",
        "id": "99729be76fa948d5a1df22618bec96ea"
    },
    "creationDate": "2018-09-21T09:13:16-07:00",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```

Example of a request for partial updating a network credential, using JSON Patch Query.

### Request

```
PATCH /credential/9fd97c82b4bf4fe7bcbee314d811290b
Content-Type: application/json-patch-query+json

[
  {
    "op": "remove",
    "path":
"/relatedContactMedium?contactMedium.id=116aca1739db4a57a9fbaebd0210b996"
  }
]
```

### Response

```
200
```

```
{
    "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/networkCredential/9fd97c82b4bf4fe7bcbee314d811290b"
,
    "id": "9fd97c82b4bf4fe7bcbee314d811290b",
    "@type": "NetworkCredential",
    "@baseType": "Credential",
    "state": "Active",
    "validFor": {
        "startDateTime": "2018-09-21T23:20:50.52Z"
    },
    "trustLevel": "high",
    "resource": {
        "@type": "ResourceRef",
        "id": "99729be76fa948d5a1df22618bec96ea"
    },
    "creationDate": "2018-09-21T09:13:16-07:00",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```


Example of a request for fully updating an entire token credential.

### Request

```
PATCH /credential/7ef64b30fd5345ac9ab9554798c21f5c
Content-Type: application/json

{
    "@type": "TokenCredential",
    "login": "google.id:107691503500061507151130823 67",
    "tokenCredential":
"6nxugrzcv0e4se81kufqf0nn0rpygf4yqzyp7gha68wgqdpm057lx97jiiy6fdpq"
}
```

### Response


```
200

{
    "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/tokenCredential/7ef64b30fd5345ac9ab9554798c21f5c",
    "id": "7ef64b30fd5345ac9ab9554798c21f5c",
    "@type": "TokenCredential",
    "@baseType": "Credential",
    "state": "Active",
    "validFor": {
        "startDateTime": "2018-09-21T23:20:50.52Z",
        "endDateTime": "2018-10-21T23:20:50.52Z"
    },
    "trustLevel": "high",
    "login": "google.id:107691503500061507151130823 67",
    "tokenCredential":
"6nxugrzcv0e4se81kufqf0nn0rpygf4yqzyp7gha68wgqdpm057lx97jiiy6fdpq",
    "creationDate": "2018-09-21T09:13:16-07:00",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
```

```
}
```

Example of a request for partial updating a token credential, using MERGE Patch.

### Request

```
PATCH /credential/7ef64b30fd5345ac9ab9554798c21f5c
Content-Type: application/merge-patch+json

{
    "@type": "TokenCredential",
    "login": "google.id:107691503500061507151130823 67",
    "tokenCredential":
"6nxugrzcv0e4se81kufqf0nn0rpygf4yqzyp7gha68wgqdpm057lx97jiiy6fdpq"
}
```

### Response

```
200

{
    "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/tokenCredential/7ef64b30fd5345ac9ab9554798c21f5c",
    "id": "7ef64b30fd5345ac9ab9554798c21f5c",
    "@type": "TokenCredential",
    "@baseType": "Credential",
    "state": "Active",
    "validFor": {
        "startDateTime": "2018-09-21T23:20:50.52Z",
        "endDateTime": "2018-10-21T23:20:50.52Z"
    },
    "trustLevel": "high",
    "login": "google.id:107691503500061507151130823 67",
    "tokenCredential":
"6nxugrzcv0e4se81kufqf0nn0rpygf4yqzyp7gha68wgqdpm057lx97jiiy6fdpq",
    "creationDate": "2018-09-21T09:13:16-07:00",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```

Example of a request for partial updating a token credential, using JSON Patch.

### Request

```
PATCH /credential/7ef64b30fd5345ac9ab9554798c21f5c
Content-Type: application/json-patch+json

[
  {
    "op": "replace",
    "path": "/login",
    "value": "google.id:107691503500061507151130823 67"
  },
  {
    "op": "replace",
    "path": "/tokenCredential",
```

```
    "value": "6nxugrzcv0e4se81kufqf0nn0rpygf4yqzyp7gha68wgqdpm057lx97jiiy6fdpq"
  }
]
```

### Response

```
200

{
    "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/tokenCredential/7ef64b30fd5345ac9ab9554798c21f5c",
    "id": "7ef64b30fd5345ac9ab9554798c21f5c",
    "@type": "TokenCredential",
    "@baseType": "Credential",
    "state": "Active",
    "validFor": {
        "startDateTime": "2018-09-21T23:20:50.52Z",
        "endDateTime": "2018-10-21T23:20:50.52Z"
    },
    "trustLevel": "high",
    "login": "google.id:107691503500061507151130823 67",
    "tokenCredential":
"6nxugrzcv0e4se81kufqf0nn0rpygf4yqzyp7gha68wgqdpm057lx97jiiy6fdpq",
    "creationDate": "2018-09-21T09:13:16-07:00",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```

Example of a request for partial updating a token credential, using JSON Patch Query.

### Request

```
PATCH /credential/7ef64b30fd5345ac9ab9554798c21f5c
Content-Type: application/json-patch-query+json

[
  {
    "op": "remove",
    "path": "/contactMedium?contactMedium.id=116aca1739db4a57a9fbaebd0210b996"
  }
]
```

### Response

```
200

{
    "href": "https://serverRoot/tmf-
api/digitalIdentityManagement/v5/tokenCredential/7ef64b30fd5345ac9ab9554798c21f5c",
    "id": "7ef64b30fd5345ac9ab9554798c21f5c",
    "@type": "TokenCredential",
    "@baseType": "Credential",
    "state": "Active",
    "validFor": {
        "startDateTime": "2018-09-21T23:20:50.52Z",
        "endDateTime": "2018-10-21T23:20:50.52Z"
```

```
    },
    "trustLevel": "high",
    "login": "google.id:107691503500061507151130823 67",
    "tokenCredential":
"6nxugrzcv0e4se81kufqf0nn0rpygf4yqzyp7gha68wgqdpm057lx97jiiy6fdpq",
    "creationDate": "2018-09-21T09:13:16-07:00",
    "lastUpdate": "2018-09-21T23:20:50.52Z"
}
```


## Deletes a Credential

**DELETE /credential/{id}**

### Description

This operation deletes a Credential entity.

### Usage samples

Example of a request to delete a specific credential.

### Request

```
DELETE /credential/754ea8ed4bef49d78ca2ba3f953cd65f
Content-Type: application/json
```

### Response

```
204
```

# API NOTIFICATIONS

For every single of operation on the entities use the following templates and provide sample REST notification POST calls.

It is assumed that the Pub/Sub uses the Register and UnRegister mechanisms described in the REST Guidelines reproduced below.

## Register listener

### POST /hub

### Description

Sets the communication endpoint address the service instance must use to deliver information about its health state, execution state, failures and metrics. Subsequent POST calls will be rejected by the service if it does not support multiple listeners. In this case DELETE /api/hub/{id} must be called before an endpoint can be created again.

### Behavior

Returns HTTP/1.1 status code 204 if the request was successful.

Returns HTTP/1.1 status code 409 if request is not successful.

### Usage Samples

Here's an example of a request for registering a listener.

### Request

```
POST /api/hub

Accept: application/json

{
    "callback": "http://in.listener.com"
}
```

### Response

```
201

Content-Type: application/json

Location: /api/hub/42

{
    "id":"42",
    "callback": "http://in.listener.com",
    "query":""
}
```

## Unregister listener

### DELETE /hub/{id}

### Description

Clears the communication endpoint address that was set by creating the Hub..

### Behavior

Returns HTTP/1.1 status code 204 if the request was successful.

Returns HTTP/1.1 status code 404 if the resource is not found.

### Usage Samples

Here's an example of a request for un-registering a listener.

### Request

```
DELETE /api/hub/42

Accept: application/json
```

### Response

```
204
```

## Publish Event to listener

### POST /client/listener

### Description

Clears the communication endpoint address that was set by creating the Hub.

Provides to a registered listener the description of the event that was raised. The /client/listener url is the callback url passed when registering the listener.

### Behavior

Returns HTTP/1.1 status code 201 if the service is able to set the configuration.

### Usage Samples

Here's an example of a notification received by the listener. In this example "EVENT TYPE" should be replaced by one of the notification types supported by this API (see Notification resources Models section) and EVENT BODY refers to the data structure of the given notification type.

### Request

```
POST /client/listener

Accept: application/json

{
    "event": {
        EVENT BODY
    },
    "eventType": "EVENT_TYPE"
}
```

### Response

```
201
```

For detailed examples on the general TM Forum notification mechanism, see the TMF REST Design Guidelines.

# Acknowledgements

## Version History

| Version Number | Date Modified | Modified by: | Description of changes |
|---|---|---|---|
| 5.0.0 | 06-Mar-2023 | Rajesh Sinha, Jio | Initial revision of the document. |
| 5.0.0 | 11-Jul-2023 | Bruno Fernandes | AP-4544 Digital identity credential and contact medium improvements. |
| 5.0.0 | 04-Mar-2024 | Bruno Fernandes | AP-4739, AP-4830, AP-4831 Accelerate Lisbon 2024 action items implemented. |
| 5.0.0 | 08-Oct-2024 | Bruno Fernandes | Fixed examples according to new API tooling linter. |

## Release History

| Release Number | Release Status | Date | Release led by: | Description |
|---|---|---|---|---|
| 5.0.0 | Preview | 14-Nov-2024 | Bruno Sousa Fernandes (NOS) | Initial revision of the document. |

## Contributors to Document

This document was prepared by the members of the TM Forum API Project team:

| Name | Company | Role |
|---|---|---|
| Bruno Fernandes, bruno.sfernandes@nos.pt | NOS, PT | Author |
| Jonathan Goldberg, jonathan.goldberg@amdocs.com | Amdocs, IL | Reviewer |
| Olivier Arnaud, olivier.arnaud@orange.com | Orange, FR | Additional input |
| Pierre Gauthier, pgauthier@tmforum.org | TM Forum | Reviewer |
| Rajesh Sinha, rajesh.ra.sinha@ril.com | Jio, IN | Author |