ACCIONES RELACIONADAS CON ALASTRIA ID

En este documento se describen las acciones relacionadas con Alastria Id.

- Asunciones
- Creación de Alastria Id
- Autenticación
- Acciones relativas a Claves Publicas
  - Creación, registro, revocación y borrado
- Acciones relativas a Testimonios
  - Emisión, registro, revocación y borrado
- Acciones relativas a Alegaciones
  - Entrega, registro, aceptacióny borrado
- Gateway
  - Transacciones genéricas
- Recuperación de claves privadas

Asunciones

Los nodos de Alastria son permisionados y por tanto no es posible iniciar ninguna interacción con la blockchain desde el exterior. Es necesaria una pieza de arquitectura que actue como Gateway (GW) que será gestionada en combinación con los nodos y por los mismos actores. Los usuarios finales necesitan el apoyo de los socios que operan un nodo y GW para todas las acciones. El GW permite detectar y gestionar posibles ataques de denegación de servicio y permite especificar las funciones disponibles.

A continuación se describen paso a paso cada una de las acciones.

Creación de Alastria Id

1. Creación en el dispositivo del usuario del par de claves personales (pública/privada).
2. Identificación ante los sistema tradicionales (off chain) del socio y selección de opción de creación de identidad Alastria.
   1. El SP genera un objeto JSON con formato AT (Alastria Token) que permita enlazar esta identificación con el paso siguiente.
   2. El SP solicita al usuario la llave pública de usuario (Generada en el punto 1).

Modelo de datos objeto JSON:

```
{
  URLGateWay  : http:www.gateway_socio.com
  URLCallBack : http:www.backend_service_provider.com/callback //Opcional
  AlastriaIDServiceProvider : 0xServiceProvider
}.firma_service_provider
```

El SP manda una notificación Push al móvil del usuario o presenta un QR que es escaneado por el móvil

3. Creación de Alastria ID por el usuario, enviando al GateWay un Alastria Identity Creation (AIC) con los siguientes datos:
    1. Objeto de transacción Ethereum para creación de Identidad

```
{
From: 0xCuentaUsuario,
To: 0xMetaIdentityManager,
Value: empty,
Data: PayloadBytes
//createIdentityWithCall(0xCuentaUsuario,AlastriaIDServiceProvider,0xRegistry

}.FirmaCuentaUsuario
//Payload llamada a registry
Data: registry.SetPubKey(HashPubKeyCuentaUsuario)
```

    2. Objeto AT enviado al usuario desde el serviceProvider (Paso 2)
    3. Clave pública del usuario (PubKeyCuentaUsuario)

El objeto Alastria Identity Creation se envía firmado con la PrivKeyUser

4. El GateWay verifica:
    1. Comprueba la firma de todos los elementos firmados
    2. Existe sesión en la capa OAuth
    3. Que la petición viene autorizada por un service provider capaz de crear identidades (para el MPV será una lista blanca)
    4. Si ya existe otro Alastria ID para ese usuario (*0xCuentaUsuario*) no se crea otra identidad y se devuelve la existente
5. El GateWay manda la transaccion del punto 3 a IdentityManager
6. El GW devuelve el alastria_id creado al sistema tradicional del socio así como a la aplicación móvil junto con otros parámetros necesarios de la red (direcciones de contratos, lista de gw, ...).
7. El socio liga el nuevo Alastria ID con el identificador corporativo,para poder usarlo directamente en autenticaciones siguientes.

Autenticación con Alastria Id

1. Acceso a WebApp y selección de Alastria Id como identificación, iniciando la creación de la sesión.
    1. Se genera un objeto JSON con formato AT (Alastria Token) que permita enlazar esta identificación con el paso siguiente.
    2. Se solicita al usuario la PubKeyUser y AlastriaID de usuario
2. Comprobación de la identidad de la aplicación del SP por la Aplicación Alastria.
    1. Solicitud de la clave publica de la aplicación (Aplicación Alastria -> GW -> getPubKey(AlastriaIDServiceProvider)
    2. Verificación de la firma del AT
3. El usuario manda un AlastriaSesion (JSON firmado) de aceptación de sesion a *URLCallBack* conteniendo:
    1. Objeto AT enviado al usuario desde el serviceProvider

2. AlastriaId del Usuario
3. Clave pública del usuario (PubKeyUser)

El objeto AlastriaSesion va firmado con la PrivKeyUser

4. El ServiceProvider recupera el Hash de PubKeyUser del Registry getPubKey(AlastriaIDUser)
5. Comprobación de la clave publica y firma del usuario y por tanto de su Identidad.
6. Si es la primera vez que se accede con AlastriaId puede ser necesario ligarlo con la cuenta en el sistema del proveedor de servicios:
    1. Utilizando usuario/password u otro sistema de autenticación
    2. Pidiendo atributos básicos (Nombre/apellidos, DNI) del nivel (LoA) que se considere (p.e.: 2 ó 3)
7. Envío del token de sesión a la aplicación Web.

Acciones relativas a Claves Públicas

Creación

Las claves publicas PubKeyUser y privadas PrivKeyUser se crearán en la aplicación Alastria en el móvil y la privada no saldrá nunca del móvil siendo almacenada en un enclave seguro. Las claves de los asociados serán creadas y custodiadas por ellos.

Registro

El usuario manda una transaccion a traves del GW y el identitymanager/proxy al AlastriaPublicKeyRegistry.set para que se registre la clave pública con los siguientes datos:

1. publicKey: Hash (pubKeyUser)

La transacción se envía firmada por la PrivKeyUser. El registro de una clave implica la inmediata revocación de la clave anterior si existe.

Revocación

El usuario manda una transaccion a traves del GW y el identitymanager/proxy al AlastriaPublicKeyRegistry.revokePublicKey para que se registre la revocación de la clave (el fin de su vigencia), con los siguientes datos:

1. publicKey: Hash (pubKeyUser)

La transacción se envía firmada por la PrivKeyAttester

Borrado

El usuario manda una transaccion a traves del GW y el identitymanager/proxy al AlastriaPublicKeyRegistry.deletePublicKey para que se registre el borrado de la clave, se indica el fin de su vigencia y que los datos firmados con dicha clave deben dejar de usarse, con los siguientes datos:

1. publicKey: Hash (pubKeyUser)

La transacción se envía firmada por la PrivKeyUser

Acciones relativas a Testimonios

Emisión (offchain)

1. Identificación del usuario ante sistema tradicional del socio mediante AlastriaId (Creación o autenticación)
2. Creación de testimonios firmados por el SP para cada atributo
    1. Consulta de datos validados del usuario en el sistema tradicional.
    2. Generación de un testimonio firmado en formato JSON firmado por el SP para cada uno de los datos validados: signedAttestment
    3. Envío de cada testimonio al móvil del usuario.
    4. Almacenamiento de los testimonios deseados en el repositorio accesible exclusivamente por el usuario, se cifrará con la clave pública del usuario (PubKeyUser). Para cada Testimonio generará una URI.

El formato del testimonio es un JSON firmado por la PrivKeySP

Registro

El usuario manda una transaccion a traves del GW y el identitymanager/proxy al AlastriaAttestationRegistry.set para que se registre el testimonio con los siguientes datos:

1. dataHash: Hash (SignedAttestment)
2. URI: Localizador abstracto del testimonio en su repositorio.

La transacción se envía firmada por la PrivKeyUser

Revocación

El Testimoniador manda una transaccion a traves del GW y el identitymanager/proxy al AlastriaAttestationRegistry.revokeAttestation para que se registre la revocación del testimonio con los siguientes datos:

1. revHash: Hash (signedAttestment + AttestmentSignature)
2. Status: askIssuer or Revoked

La transacción se envía firmada por la PrivKeyAttester

Borrado

El usuario manda una transaccion a traves del GW y el identitymanager/proxy al AlastriaAttestationRegistry.deleteAttestation para que se registre el borrado del testimonio con los siguientes datos:

1. dataHash: Hash (signedAttestment)

La transacción se envía firmada por la PrivKeyUser

Acciones relativas a Alegaciones

Presentación o entrega

1. El usuario y la aplicación del SP están mutuamente identificados mediante autenticación Alastria
2. El SP crea una solicitud de datos (solicitud de Claim), conteniendo:

1. La lista de atributos requeridos (identificados mediante el esquema de nombrado y el nombrel del atributo), con el nivel EIDAS requerido de cada uno.
2. El callback donde deben ser enviados los datos.

La petición tiene formato JSON firmado por PrivKeySP.

3. El SP envía la solicitud de datos al usuario mediante:

    1. URL inter aplicación.
    2. Push notification al móvil.
    3. Código QR para escanear con la aplicación Alastria del móvil.

4. La Aplicación Móvil Alastria valida la solicitud (comprobación de firma) y realiza las siguientes acciones:

    1. La aplicación selecciona los testimonios más adecuados.
    2. Se los presenta al usuario para su validación.
    3. Permite que el usuario cambie la elección pre-definida.
    4. Permite la aprobación/rechazo de la solicitud.

5. Remisión del callback con la respuesta:

    1. Rechazo.
    2. Aprobación: envío de un Claim con los testimonios elegidos El formato es un JSON firmado por PrivKeyUser

6. Se almacena la Alegación en el repositorio de forma que sólo el usuario pueda acceder, cifrándola con la PubKeyUser. Para cada Testimonio generará una URI.

Registro

El usuario registra el Claim enviado a traves del GW y el identitymanager/proxy al AlastriaClaimRegistry.set para que se registre el claim con los siguientes datos:

1. subjectHash: Hash (SignedClaim)
2. URI: Localizador abstracto del testimonio en su repositorio.

La transacción se envía firmada por la PrivKeyUser

Aceptacion

El ServiceProvider manda una transaccion a traves del GW y el identitymanager/proxy al AlastriaClaimRegistry.confirm para que se registre la recepción del Claim con los siguientes datos:

1. SPHash: Hash (SignedClaim + claimSignature)

La transacción se envía firmada por la PrivKeySP

Borrado

El usuario manda una transaccion a traves del GW y el identitymanager/proxy al AlastriaClaimRegistry.deleteClaim para que se registre el borrado del Claim con los siguientes datos:

1. dataHash: Hash (SignedClaim)

La transacción se envía firmada por la PrivKeyUser

Gateway

El Gateway presentará una interfaz REST y recibirá los parámetros en formato JSON firmado por el emisor de la transacción (PrivKeyUser). Realizará simpre las siguientes validaciones genéricas, adicionales a las indicadas en cada una de las operaciones anteriores.

1. Existencia de la cuenta del emisor (excepto en la creación de AlastriaID)
2. La firma del emisor.
3. Que el destinatario de la transacción es el identityManager

Transacciones genéricas

Cuando una aplicación de un SP propone a un usuario que invoque un contrato, la aplicación generará un JSON firmado, con los siguientes datos:

1. Transacción completa a firmar por el usuario, preparada para ser enviada a traves del IdentityManager/Proxy al contrato destino.
    1. Dirección del contrato destino
    2. Función a invocar en el contrato.
    3. Valores de los parámetros.
2. Descripción amigable de lo que se está solicitando.
3. Callback de respuesta.

La propuesta de transacción es firmada por ProvKeySP.

La aplicación comprueba la firma y presenta la descripción amigable, junto con los datos de la transacción para su aceptación o rechazo. En caso de aprobación, se firma la transacción y se remiten los datos a través del Gateway y el metaidentitymanager/proxy al contrato destino.

Se incorporarán controles sobre las transacción (por ejemplo, que no se trate de ninguno de los contratos relacionados con identidad), etc.

Tras la invocación de la transacción, el Gateway envía el hash de la transacción a la Aplicación Móvil Alastria. El móvil envía a la url de callback el hash de la transacción.

TBD: Posible registro de la propuesta de transacción y la transacción en el Registry (hash propuesta, hash transacción)

Recuperación de identidad y claves privadas

Sustitución de las claves de control disponiendo de la clave actual

Esta opción es útil para sustituir la PrivKeyUser de forma periódica o cuando se suponga que la clave privada ha podido ser comprometida, pero se conserva. El IdentityManager puede cambiar la asociación entre la antigua clave privada y la nueva y registra la nueva clave publica en el registry.

Debe recuperarse toda la información cicfrada del repositorio y cifrarse de nuevo con la nueva clave pública. Si se considera que la antigua clave privada ha estado comprometida, se podria solicitar la marca de borrado en la clave publica correspondiente.

Recuperación de claves privada y pública perdidas

Se contempla así mismo un mecanismo de salvaguardia y recuperación de la clave personal, publica y privada, del usuario.

Cada clave se troceara en n partes (al menos 3) de forma que se pueda reconstruir la clave original con cualesquiera n-1 partes mediante la técnica de Shamir Secret Sharing. La partes se cifrarán con una password del usuario y se repartirán entre n socios para su salvaguardia. Los socios podrán ser elegidos por el usuario pero se le propondrán 3 socios de los que estén en la lista blanca de creación de identidades o hayan prestado al menos n testimonios de nivel 2-3, en caso de no existir al menos tres socios que cumplan la condición se dará un aviso al usuario.

Proceso

1. La recuperación de la clave la iniciará el usuario mediante un (nuevo) dispositivo con la aplicación Alastria instalada.
2. Identificación ante los sistema tradicionales (off chain) del socio y selección de opción de recuperación de claves Alastria.
    1. Se genera un Alastria Token.
    2. Se entrega el Alastria Id correspondiente al usuario identificado y la parte de las claves que almacena el SP.
3. Se repetirá el proceso hasta obtener n-1 partes de las claves
4. Con las n-1 partes la Aplicación Móvil Alastria pedirá el password al usuario para recomponer y descifrar el par de claves, instalandolas en el enclave.

En este punto se podría comprobar que el registro de la clave publica en el registry coincide. Se recomienda fuertemente realizar los pasos indicados en el caso anterior sustituyendo la clave recuperada por una nueva.

Pérdida total de las claves

En caso de pérdida de la clave privada del usuario el identity manager es capaz de restablecer la relación entre una nueva pareja de claves y el contrato proxy que constituye el AlastriaId.

Se contempla que dicha restitución se realice mediante el concurso de 3 o más asociados que hayan sido previamente seleccionados por el usuario y que pertenezcan a la lista blanca de creación de identidades. Se está analizando si la participacióin de la FNMT en Alastria puede abrir otras opciones complementarias.

Se mantiene la identidad pero se habrán perdido los testimonios y alegaciones del repositorio salvo que se disponga de un backup.

Documentacion asociada

Formatos de intercambio

Diagramas de tiempo