Device Trust and User Authentication using DID and Blockchain for Second-Factor VPN Access

Overview

To replace Entrust PKI and implement a second-factor authentication for users before VPN access, this design explores the use of Decentralized Identity (DID) and blockchain anchoring. This ensures that both the user and the device are verified before accessing the network, enhancing security by tying device trust to user credentials.

Solution Components

```
graph TD
    subgraph User Device
    A[Device Generates DID]
    end

    subgraph Org System
    B[Org System Issues Device Credential]
    end

    subgraph Blockchain
    C[Blockchain Anchors DID and Credential]
    end

    D[User Logs In]
    E[Credential Verified]

    A --> B
    B --> C
    D --> A
    D --> E
    E --> C
```

1. Device Issuance of a DID

Devices (laptops, smartphones, etc.) can be issued their own DID by your organization's identity provider. The device’s DID is stored in a secure storage area (e.g., Trusted Platform Module (TPM)) and linked to the user's DID.

- **Device DID Creation**: The device generates a unique DID tied to hardware identifiers (e.g., MAC address, TPM keys).
- **Linking Device to User**: The device's DID is linked to the user’s DID, establishing a trust chain between the device and the user.

2. Device Credential Issuance

Once the device generates a DID, it receives a credential from a trusted authority (e.g., your IT department). The credential contains:

- Device ownership (linked to the user's DID)
- Hardware information (to ensure device uniqueness)
- Security posture (ensuring compliance with required standards)

```
graph TD
    A[Device Generates DID]
    B[Org Issues Credential to Device]
    C[Device Receives Credential]
    D[Credential Anchored on Blockchain]

    A --> B
    B --> C
    C --> D
```

3. Device Authentication and Verification Process

During user login or VPN access, the device proves it holds the correct DID and credential in a challenge-response process:

- The device sends its DID and credential to the server.
- The server verifies the credential against the blockchain or decentralized network.
- The server checks that the device’s DID is linked to the user’s DID, ensuring that only trusted devices for a specific user are authorized.

```
sequenceDiagram
    participant User Device
    participant Auth Server
    participant Blockchain

    User Device->>Auth Server: Sends DID and Credential
    Auth Server->>Blockchain: Verifies Credential
    Blockchain-->>Auth Server: Validates Credential
    Auth Server-->>User Device: Success or Failure Response
```

4. Blockchain Anchoring

Blockchain provides the trust anchor for device verification. Device credentials and their verification details are recorded immutably on a blockchain, ensuring tamper resistance and an additional trust layer.

```
graph LR
    A[Device Credential Issued]
    B[Blockchain Ledger]
    C[Credential Anchored to Blockchain]

    A --> C
    B --> C
```

5. Second-Factor Authentication with Device Trust

After verifying the device, a second-factor authentication is required for further security:

- **Device + User Credential**: Both the device’s DID and the user's DID are challenged for verification.
- **MFA or Verified ID on a Separate Device**: A second factor, such as a push notification, biometric authentication, or Verified ID on a mobile device, can be used to verify the user.

```
sequenceDiagram
    participant User Device
    participant Auth Server
    participant User Mobile
    User Device->>Auth Server: Device and User DID
    Auth Server->>User Mobile: MFA Challenge (Push or Verified ID)
    User Mobile-->>Auth Server: MFA Response
    Auth Server-->>User Device: Access Granted
```

Benefits of DID-Based Device Trust

- **Device Ownership Verification**: Only devices with valid, linked DIDs are trusted.
- **User and Device Linkage**: Ensures that only authorized devices for a specific user can access resources.
- **Tamper-Resistance**: Blockchain anchoring prevents credential tampering.
- **Revocation and Monitoring**: Device credentials can be revoked and tracked via blockchain, with immediate effect.

Available Solutions

1. Microsoft Entra Verified ID for Devices

Entra Verified ID allows the issuance of custom credentials for both users and devices. This integrates with existing infrastructure like Azure AD for enforcing conditional access policies.

2. Trusted Platform Module (TPM) with DID

TPM-equipped devices can securely store DIDs and perform secure, signed transactions for authentication.

3. Third-Party DID Solutions

Solutions like **Hyperledger Indy** or **Sovrin** support DID and blockchain-based device management.

Example Workflow for Device Verification

1. **Device Registration**

    - Device generates a DID.
    - Organization issues a credential linking the device to the user.

```
sequenceDiagram
    participant User Device
    participant Org System
    participant Blockchain

    User Device->>Org System: Generates DID and Requests Credential
    Org System->>Blockchain: Anchors Credential to Blockchain
    Blockchain-->>Org System: Confirms Credential Anchored
    Org System-->>User Device: Credential Issued
```

2. **Login Process**

    - User logs into the device.
    - Device presents its DID and credential to the authentication server.
    - Server verifies the credential via blockchain and checks the device-user DID linkage.
    - Upon verification, the user is challenged with a second factor (e.g., MFA or Verified ID on a phone).

```
sequenceDiagram
    participant User Device
    participant Auth Server
    participant Blockchain

    User Device->>Auth Server: Presents DID and Credential
    Auth Server->>Blockchain: Verifies Credential Anchoring
    Blockchain-->>Auth Server: Confirms Credential Validity
    Auth Server-->>User Device: Grants Login Access
```

3. **VPN Access**

    - After verifying both the device and user, VPN access is granted.

```
sequenceDiagram
    participant User Device
    participant VPN Server
    participant MFA Service

    User Device->>VPN Server: Requests VPN Access with DID
    VPN Server->>MFA Service: Initiates Second-Factor Challenge
    MFA Service->>User Mobile: Sends MFA Challenge
    User Mobile-->>MFA Service: Confirms MFA Response
    MFA Service-->>VPN Server: Grants Access
    VPN Server-->>User Device: VPN Access Granted
```

Summary

By using DID and blockchain anchoring, you can implement a robust solution that verifies both the user and the device, ensuring secure, authorized access to your network. Blockchain provides a tamper-proof trust layer, and Microsoft Entra Verified ID can be extended to incorporate device credentials for enhanced security and seamless second-factor authentication.

```
This markdown file contains all the requested information and includes Mermaid.js
diagrams under the appropriate sections. The diagrams visualize the flows for
system-to-system interactions and user interactions throughout the authentication
and verification process. Let me know if you need further adjustments!
```