Australian Banking Association

CDR Data Holders outbound connection whitelisting

This paper presents the CDR Data Holders (banking) concerns and proposed solutions regarding outbound connection whitelisting.

Problem

As per the Consumer Data Right (**CDR**) Register Standards, Accredited Data Recipient (**ADR**) software products will dynamically register with one or more data holders to obtain client credentials used to retrieve consumer data on behalf of a consumer. Upon receiving the request to register a new software product or to update a registration request from the ADR, data holders are required to validate the request JWT (JSON web token), and the SSA (software statement assertion) embedded within it before responding with the client credentials. The signature of the JWT is validated by referencing the ADR's JWKS (JSON web key set) URI available in the SSA.

These standards pose an implementation challenge for the data holders which impacts the security of their environments. This is due to security practices followed by data holders requiring all external network connections to be individually identified and whitelisted on server/appliances (like firewall, proxies, etc.) which handle the outbound internet connections from internal applications and services. These whitelisting policies on forward proxies restrict or permit internet connections for applications and internal users. As a standard security practice, user connections to websites are permitted based on categorisation and reputation scores. However, internet connections made by applications are explicitly whitelisted with a known URIs. This is a standard adopted by organizations (including many data holders) with mature security posture and it acts as an effective security control by mitigating against data exfiltration risk from Data Holder environment (like in case of malware sending data to a malicious unknown URI).

As per the current standards, the URIs to retrieve the JWKS and the sector_identifier_uri are not known to the data holder prior to receiving the registration request, as it is only provided in the SSA which is embedded within the request. Additionally, the ADR registration request is classified under High Priority tier with response time of 1000ms.To be complaint with the standard, the data holder has to bypass the whitelisting control by allowing unrestricted internet access from the internal application/service, in order for the data holder's internal service to discover the ADR URIs, retrieve the JWKS, and dynamically register the ADR within the acceptable response times.

Granting unrestricted internet access to internal services results in an elevated level of data breach risk within the data holder environment. For example, an attacker could potentially exploit an undiscovered vulnerability on this service/application that has unrestricted internet access and ex-filtrate CDR or other data through this exit route. Another is example is a compromised system connecting to external command and control server. URL/Domain whitelisting to allow connections to only known URIs on the server/appliances (like firewall, proxies or etc.) of the data holder's network perimeter serves as a robust and a cost-effective control to mitigate this risk.

Outbound connection whitelisting is a common security control which is used as a part of multi-layered defence strategy and considered to be a part of the best practices. MITRE ATT&CK® is widely used globally-accessible knowledge base of adversary tactics and techniques. It covers filtering of network traffic as one of the risk mitigation techniques: https://attack.mitre.org/techniques/T1090/.

Proposed options:

Option 1: Notification to Data holders prior to registration (process change only, no technology change required)

CDR register to notify the data holders the intent of registration and provide the necessary URIs upfront (at an agreed pre-defined timeframe), so that the data holder can perform configurations required for

successful registration. This communication could take place in existing offline channels using the CDR incident management system.

This option does not require additional technical implementation by either data holders or ADRs and can be implemented without any additional lead time. The data holders will continue to trust the JWKS URI and the sector_identifier_uri present in the SSA, but the notification will assist the data holder to whitelist the ADR endpoints prior to receiving the registration request.

Implementation impact:

- **Data Holders:** None. Optional whitelisting for Data Holders as per current process (if required).
- **Data Recipients:** None.
- **CDR Register:** None. Non-automated notification to Data Holders.

Change to the standards: Low.

Operational Overhead: High (manual process involving CDR register and DH communication for every registration).

Implementation time: Could be implemented **immediately**.

Option 2: Make the domain/URIs available in the register API.

This option requires changes to the CDR register APIs to provide the list of domain/URIs of the ADR as part of the Register APIs. Currently, Data Holders access the Register APIs to update the data holder cache periodically as per the Metadata Cache management standards. By providing the URIs of the ADRs upfront before they become active, the data holders will have an opportunity to perform necessary configurations required for the Dynamic Client registration to be successful.

As part of the registration process, the Data Holder will still continue to trust the JWKS and sector_identifier_uri from the SSA over the domain/URIs received from the Register API.

Implementation impact:

- **Data Holders:** optional change for Data Holders that require whitelisting of outbound connections. Allowance for manual or fully automated process on Data Holder side.
- **Data Recipients:** None.
- **CDR Register:** Additional field to be added to an existing API.

Change to the standards: Low.

Operational Overhead: Low (no additional overhead added to the end-end DCR flow).

Implementation time: Medium (minor changes are required to the CDR register and for Data Holders).

Option 3. A new secure API endpoint hosted by the CDR Register

This option requires a new authenticated endpoint hosted by the CDR Register which can be accessed by the Data holders to fetch the ADR's JWKS and the sector_identifier_uri in the SSA prior to ADR submitting the registration request. As this is a new authenticated flow in the CDR eco-system, standards will have to be developed for Data Holder authenticating to CDR Register.

As part of the registration request, the data holder could rely on the URIs fetched from this new API or from the SSA.

Implementation impact:

- **Data Holders:** optional change for Data Holders that require whitelisting of outbound connections. Allowance for manual or fully automated process on Data Holder side.
- **Data Recipients:** None.

- **CDR Register:** new secure API based on existing API with additional field.

Change to the standards: High.

Operational Overhead: Low (no additional overhead added to the end-end DCR flow).

Implementation time: Medium.

Option 4. JWKS endpoints hosted by the CDR Register

This option CDR Register to capture Data Recipient's JWKS during on-boarding, allow ongoing JWKS management and host JWKS endpoints for access by data holders. This removes the requirement of additional whitelisting for JWKS access and Dynamic Client Registration.

No ongoing URL whitelisting is required for new participants.

Implementation impact:

- **Data Holders:** Re-registration of ADRs (automated).
- **Data Recipients:** Update JWKS via CDR register portal, download the latest SSA and re-register with Data Holders.
- **CDR Register:** capture Data Recipient's JWKS during on-boarding, allow ongoing JWKS management and host JWKS endpoints for access by data holders.

Change to the standards: Medium.

Operational Overhead: Low (no additional overhead added to the end-end DCR flow) for Data Holders and Data Recipients. Note that there may be additional overhead introduced by the process used for securely transferring private keys between data recipients and the CDR.

Implementation time: Medium.

Note: Additional design is required for CDR custom revocation endpoint and sector_identifier_uri. This will impact the feasibility of this option. The design of the mechanism used for securely transferring private keys between data recipients and the CDR may also impact the feasibility of this option. Other potential alternatives to option 4 include:

1. Change the NFR for DCR to a more reasonable value to allow for dynamic whitelisting.
2. Remove JWT signing and high-risk fields from the DCR request and use the DCR update endpoint to transmit these fields.
3. CDR Register provides an API for ADRs to generate a signed DCR request, thereby using the CDR Register's JWKS for this request.

Recommendation from ABA:

Adopt Option 1 as a short-term solution and work on implementation of Option 2 as a medium term solution.

Consider Option 4 as a long-term solution for the ecosystem.

This staged approach allows to immediately solve potential problems for both Data Recipients and Data Holders and to provide a pathway to a fully automated process of whitelisting for Data Holders that require it.