IAM Connect Token Exchange – Security commitment

Commitment

An integrator playing the role of a "Trusted Platform" must also sign and abide by the Annex A – Security commitment from the Trusted Platform document.*

In addition, usage of IAM Connect Token Exchange service is subjected to the specific rules mentioned below.

1. Exchange and limited delegation

Authorisation tokens are generally <u>non-transferable</u>, they can only be submitted by the authorised presenter to the intended relying party marked as audience. If a client is required to authorise follow-up calls to other services to handle the original request, he must do so with an exchanged token with the correct updated audience and authorised presenter and not with the original token.

In order to exchange tokens for clients that require the user's consent, this consent must be registered prior to the exchange request.

A request for exchanged tokens can never exceed the capabilities of the original token it is based upon.

It is assumed that exchanged tokens have a short lifespan and cannot be renewed.

2. Communications

All tokens must be used as intended as authorisation headers of an HTTPS connection and for the sole purpose of authorising requests.

It is the responsibility of the caller of a service to ensure data minimisation by actively seeking to limit the capabilities and information available in the token sent to that service. For example, if a target service should be unaware of the user's real identity or could abuse some capabilities, then that service must be called with an exchanged token that has lost that capability and pseudonymises the user. Calling a target with wider capabilities than they expect is a privilege escalation, calling a target with data about the user that it is not intended to receive or actively refuses to process is a data breach.

An exchanged token can only be used to serve the request authorised by the original token. They should not be used out of sequence of a legitimate request, offline or without intent from the original user. Every usage of those digital keys is always on behalf of the user, and the incoming request is the mandate allowing it's usage.

3. Data

Original and exchanged tokens should be deleted from storage or memory as soon as they expire.

Correspondence between the original token and the exchanged token must be kept confidential. Integrity protection is also essential to ensure the wrong token is never used.

No attempts will be made to cache tokens or correlate token field values with other data, user information or subsequent visits beyond the need to serve the incoming request. This is especially true for values that are intended to protect the user's identity such as pairwise identifier or pseudonyms.

Exchanged tokens are secondary credentials representing a delegation of rights from an end user; they must be protected during their validity period as an asset requiring the highest level of confidentiality protection.

4. Incidents

Any incident such as a data breach, loss or compromise of credentials must be immediately reported and disclosed to the eHealth DPO (*dpo@ehealth.fgov.be*) so that counter-measures (such as revoking or rotating credentials) can be taken. Incident management will remain trusted platform's responsibility.

Sending scope or non-pseudonymised information to a target service that explicitly requires those to be removed or pseudonymised (by exchanging the token) constitute a data breach.

5. Documents

Implementers must provide a sequence diagram detailing the need for a token exchange, starting with an incoming call authorised by an original token, interactions with the Token Exchange service to obtain an exchanged token, and which changes in scope, data or audience are expected and subsequent calls issued with that exchanged token.

Implementers must briefly describe how they will manage and protect the storage of the different tokens and ensure the correct tokens are used with each calls.

Name – First name

Date

Signature