wLCG statement on acceptability of use of Identifier-Only Trust Assurance Credentials in the Infrastructure by members of the LHC experiment VOs

Update to the wLCG Policy on Approval of Certification Authorities in the context of the Federated ID & WebFTS pilot

RW,DLG,JT, SL, DPK: 28 October 2015

The wLCG MB approved inclusion of the CERN LHC IOTA CA in the context of the wLCG JSPG policy on the Approval of Certification Authorities 3.0[1] on October 27th, 2015 on the following considerations

1. Why do we propose that WLCG uses an IGTF IOTA CA?

- It is a vital part of the ongoing work plan to move away from users with X.509 certificates towards the use of federated authentication via home institutes.
- We still need X.509 certificates for consumption by WLCG services but these would be dynamically produced by a CERN Security Token Service using an IGTF IOTA CA.
- The use of the IGTF IOTA profile allows federated authentication from people without the need for face to face identity vetting. We still need to maintain the existing levels of assurance and confidence in identity vetting so we use the robust registration procedures of the LHC experiments and the CERN HR database rather than relying on the CA.
- We also need to maintain the same level of traceability back to individuals as we have today with personal certificates.

2. What are the limitations of the current technology?

- Today trust in a CA is defined per site/system and not per VO.
- For sites supporting VOs other than LHC there is therefore a large danger in generally trusting IOTA CAs. Another VO using an IOTA CA may not have the same quality of identity vetting procedures as at CERN.
- We have to develop a way of a new CERN IOTA CA only being useable by the LHC VOs. And ensure that no other IOTA CA is generally distributed in the WLCG trust anchors.

3. Proposed work-around to the limitations

- CERN acquires IGTF accreditation for their new IOTA CA.
- Deploy mechanisms ensuring only registered LHC VO users can obtain certificates from this CA.
- We also propose limiting the use cases where such authentication can be used to those reviewed and approved by the WLCG MB.

4. What are we going to ask the WLCG MB to approve/endorse?

- Endorse the general thrust of this approach
- Approve the use of the IOTA profile by WLCG, on a CA-by-CA basis and for specified applications
- Approve the use of the new CERN IOTA CA for this use case (once IGTF accredited)
- Request all WLCG sites to install the new WLCG CA Trust anchor
- Approve the specific current use case (WebFTS)
- Encourage developers of authentication software and wLCG deployment to add the capability for authorization based on the combination of VO membership and of credential issuer
- Evaluate and approve or deny any future use case

Table of Contents

[1] https://edms.cern.ch/document/428038/7

Introduction

The majority of wLCG users would benefit from expanded use of credentials based on Federated Authentication ("FedAuth") for accessing wLCG services instead of employing personal certificates either installed in browsers or used to create proxy certificates. Secure use of FedAuth on the wLCG infrastructure relies on two capabilities: a) a translation of FedAuth credentials to a form understood by the wLCG services, and b) some agreed mechanism to retain the current credential assurance levels and confidence in identity vetting.

This statement concerns a major step in the direction of user access via FedAuth. WebFTS is a file transfer and management service allowing users to manage data transfers in e.g. wLCG[2]. It can leverage FedAuth so that users can login with their home institute credentials. Capability a) above (translation) can be achieved using an on-line certification authority (CA)[3] via the STS Security Token Service[4]. This "CERN LCG IOTA CA" is not currently accepted as a trusted authority in wLCG or elsewhere[5].

However, FedAuth for Research and Education (R&E) does not yet provide assurance (b) above) equivalent to the currently acceptable trust level, in particular when viewed globally: the assurance level is very much dependent on the specific federation (country), the institution involved, and even the specific user ID. Security of these credentials (i.e. that it has not been compromised) is reasonable, but there is no consistent identity information ("what is this user actually called by name"), nor is there a guarantee that this identity is permanently assigned to only one single user. The mechanisms assured by the IGTF IOTA accreditation cover ensuring that credentials contain a unique, non-reassignable identifier, and their secure issuance based on any underlying FedAuth. For the assurance level ("who does the identifier belong to") and traceability ("how was this user vetted"), additional mechanisms are needed.

Specifically for wLCG, the relevant data are already stored in the CERN HR database and the LHC VO Management Service (VOMS) systems – and 'high-quality' identity vetting mechanisms are already in place for registering as a User at CERN in order to then be permitted to enroll in the LHC VOMS services (also using the home institute affiliation and status at CERN as stored in the CERN HR database).

Thus, a combination of the 'currently-available' R&E FedAuth, the IGTF IOTA ensured uniqueness and security thereof, and the identity vetting and traceability provided by the CERN HR database and LHC VOMS services taken together is sufficient to provide a reasonably high level of security for accessing the WebFTS service – whereas each one individually would not suffice.

Unfortunately available software today does not allow one to express "only accept an IOTA CA credential *if* the person is *also* in one of the LHC VOs". This problem is new as we so far only accepted CAs that also themselves required their subscribers to provide identity and traceability data in order to obtain a certificate. In order to enable the vision of FedAuth access in the future and hence enabling use of wLCG services by a much larger community of researchers (i.e. without the

[2] https://webfts.cern.ch
[3] https://indico.cern.ch/event/358127/contribution/7/2/material/slides/0.ppt
[4] http://www.eu-emi.eu/security-token
[5] The CERN LHC IOTA CA is also still to be accredited by the IGTF under the IOTA Authentication Profile. This is expected to be accomplished before it is to be used in the production infrastructure.

need to understand and use certificates explicitly anymore) we need to make such a coupling possible – as well as further develop better technical interoperability and more mature assurance levels.

This statement describes a trajectory to achieve the above, including an intermediate step that involves the LHC VOs as a prototype example of a VO with a high-quality membership service, deployed with compensatory controls in the form of a LHC-specific IGTF IOTA CA.

Considerations and Recommendations

Considering that

a. it is desirable to permit access to selected services with home institution credentials while prevent duplication in the user vetting and registration process;

b. the assurance provided by and the traceability of credentials based on the current R&E federations and home institutions is not homogeneous and does not in itself provide sufficient information for identifying users;

c. it is achievable to issue IGTF IOTA compliant credentials to any R&E user authenticated via eduGAIN[6];

d. the LHC experiment VO membership systems are entirely and exclusively linked to the CERN HR database;

e. the LHC experiment participants in the CERN HR database are already authenticated in a manner compliant with the IGTF BIRCH LoA[7] as they have access to the traditional user and host certificates such as issued by the already IGTF accredited[8] CERN CA today;

f. the CERN HR database, with the LHC VO management systems, can provide the necessary assurance information to complement the level provided by current R&E federations;

g. the LHC VO management systems substantially implement the assurance and operational requirements of the Guidelines for Attribute Authority Service Provider Operations[9];

h. the assurance level provide by LHC VO membership is not commonplace but significantly higher, and that therefore the suitability of IOTA credentials for non-LHC communities is not to be taken for granted;

i. there is no current support in software to make decisions based on the combination of VO membership and credential issuer;

j. the sites and services in wLCG should not diverse from peer and leveraged infrastructures, nor be required to duplicate service installations in order to maintain a constant IT security risk level;

[6] https://www.edugain.org/
[7] https://www.igtf.net/ap/loa
[8] The CERN IT/OIS CA is accredited by the EUGridPMA for the IGTF according to the MICS AP (i.e. Birch LoA)
[9] https://www.eugridpma.org/guidelines/aaops/

k. a specific CERN LHC IOTA CA can be made available by CERN that also specifically implements the requirement that its subscribers be current members of an LHC VO, and are so registered in the CERN HR database, while at the same time issuing credentials based on R&E federated log-in and being accredited under the IGTF IOTA AP;

l. that in the future, when appropriate software support is deployed in order to make combined (VO+ID-issuer) authorization decisions, the VO restrictions on the CERN LHC IOTA CA may be lifted or relaxed;

the wLCG management:

1. **envisions the acceptance** of the IGTF IOTA profile as an additional acceptable credential authority profile for wLCG, under the condition that each request for the use of a new IGTF-accredited IOTA CA in wLCG is reviewed and approved by the wLCG Management Board;

2. **reconfirms** its commitment to an integrated infrastructure, and the requirement to prevent duplication of service end-points for wLCG specific reasons;

3. **strongly encourages developers** of authentication software and the wLCG deployment groups to add the capability for authorization based on the combination of VO membership and of credential issuer and (IGTF grouped) issuer[10];

4. **endorses the use of the "CERN LHC IOTA CA"** as a specific additional trust anchor for sites and services supporting the wLCG LHC experiments as an interim measure, once it has been accredited by the IGTF under the IOTA AP;

5. **requests** that sites install the "ca-policy-lcg" trust anchor policy meta-package[11] alongside any other policy meta-packages they already install;

6. **requests** peer infrastructures and the infrastructures it leverages, in particular EGI, to continue to support the distribution of the "ca-policy-lcg" meta-package and permit conveyance of the CERN LHC IOTA CA packages in order to facilitate its distribution;

7. **will endorse the WebFTS use case, and will evaluate and approve or deny** any future use case of the CERN LHC IOTA CA, and possible wider credential availability of the CERN LHC IOTA CA with wLCG sites and with peer and leveraged infrastructures prior to their introduction;

8. **agrees to review** the *status aparte* of the CERN LHC IOTA CA, and assess availability of authorization software supporting combined (VO plus credential issuer) decisions, on a six-monthly basis;

[10] This grouping allowing a policy to express decisions like "accept LHC-VO + (any of) IOTA, Classic, MICS, or SLCS", "accept any VO + (any of) Classic, MICS, SLCS", or "deny (any VO) + IOTA"

[11] This meta-package codifies the wLCG policy, akin to what, e.g., the ca-policy-egi-core policy meta-package does for EGI. Today, this meta-package depends in turn on the ca-policy-igtf-classic, -mics, and –slcs packages. The ca-policy-lcg meta-package is today also distributed via the EGI repository (although the entire distribution is also available via https://lcg-ca.web.cern.ch/
Sites that have the 'lcg-CA' package installed (mainly those installed before 2011) will already have both policy packages (ca-policy-egi-core *as well as* ca-policy-lcg) activated.
The ca-policy-lcg package can and should be installed in addition to any other trust anchor policy packages for infrastructures in which the site participates, and in conjunction with and subject to local policy.

Rationale for the wLCG Acceptability Statement

The wLCG JSPG Policy on Approval of Certification Authorities version 3[12] considers the use of IGTF[13] Classic, MICS, and SLCS Authentication Profiles (APs) sufficient for authentication to wLCG resources and services. Accreditation of credential issuers according to these IGTF APs ensures that user identity is vetted according to good standards, that contact information is recorded, the real name of the person is known and recorded, that sufficient traceability is provided, and that the credential is issued to the proper person. The IGTF accreditation under any profile also means that the name in the credential will be persistent, unique, and never re-assigned to a different entity (making it suitable for use as an anchor for e.g. community membership databases, access control, and data ownership).

The wLCG experiments hosted at CERN are supported through a registration, vetting, and community enrolment process that ensures a reasonable level of confidence in the credential and the traceability it provides. This process is executed through the CERN User Office and technically supported through the CERN HR Database and the VO Management Services linked thereto. This process is periodically audited, and enforces by technical means compliance with documented policies. In particular this process already supports the verification of users on the basis of which certificates are issued through the IGTF MICS[14] accredited CERN CA, meaning that the users involved have presented themselves physically at the appropriate registration service, and also are Members of Personnel as defined in CERN's Administrative Circular 11[15], employees of CERN contractors, participant to an experiment, or honorary members.

Since this traceability information is already contained in the CERN HR database, has been verified, and since CERN will participate in the follow-up of incidents, there is no *a priori* reason within the wLCG to duplicate the collection of this information. This *in abstracto* means that credentials issued under the IGTF "Identifier-Only Trust Assurance" IOTA[16] accreditation level – when always used in conjunction with VO data exclusively linked to this CERN HR process – would be sufficient to provide traceability and fulfil the persistency and non-reuse requirements necessary for VO membership and for registering data ownership. They will serve merely as authenticators.

Reflection on the special character of wLCG User Registration

The traceability and vetting performed through the CERN HR system is largely unique, characteristic of highly organised, long-term communities with organic administrative staff and capabilities, and specific to the wLCG CERN LHC communities. Moreover the enrolment process used by the CERN Users Office and the LHC experiments is entirely independent of external credentials. For example, contrary to practice in many other scientific communities, the enrolment process relies exclusively on primary sources of identity (official photo-IDs, official databases, employment contracts, and in-person appearance). In this process also verified contact details are collected and stored in an auditable way.

[12] https://edms.cern.ch/document/428038/7
[13] Interoperable Global Trust Federation IGTF, see https://www.igtf.net/
[14] https://www.igtf.net/ap/mics
[15] https://cds.cern.ch/record/1754090?ln=en
[16] https://www.igtf.net/ap/iota/

This in practice means that the User Registration for the LHC experiments results in an authentication assurance level, provided through the CERN HR database, that meets or exceeds the requirements of the IGTF "BIRCH"[17] level of authentication assurance[18].

Most other communities typically use the data from electronic credentials (such as from an IGTF Classic, MICS and SLCS certificate, and the reasonable likeness of the person's name included in such a certificate) to confirm eligibility: e.g. self-registration and/or electronic mail, supported by the reasonable likeliness of the person's name and affiliation, to enroll members in their community. An IOTA credential, being pseudonymous and not linked to a verified contact address, is (intentionally) unsuitable for such a process, since the community has no independent verifiable way of obtaining this data needed for traceability.

Therefore, in order to retain end-to-end traceability and assurance, and not increase the IT security risk to which sites and services are now exposed, only those communities with a regulated and auditable enrolment process, specifically themselves providing an assurance level such as BIRCH or CEDAR[19] (such as the wLCG LHC experiments) can use IOTA credentials as authenticators.

It may be considered as a reference that, within the IT security risk envelope currently accepted by the sites, services and infrastructure of wLCG (and also of EGI), the combined level of assurance provided jointly by the community (VO) plus the identity provider (CA) should meet or exceed the IGTF assurance level BIRCH ('MICS') and/or CEDAR ('classic'). Short-lived credentials, such as used by SLCS identity providers, are not readily useful for communities, since the community life time will typically be longer than ~11 days (1 million seconds).

Acceptability of IOTA AP accredited CAs in the wLCG Trust Fabric and current limitations

Having considered the identity vetting and traceability requirements, wLCG desires to endorse the use of IGTF IOTA accredited CAs within the wLCG trust fabric, provided this can be done without impact or increased risk for the sites of wLCG and for the infrastructures which it leverages, and without necessitating a split of services at any site.

At this point in time, the necessary support in authorization software is not yet available to implement a verification at all service end-points of the association between a given (IOTA) CA and its joint LHC VO. Such software support is needed to generally accept IOTA CAs for service end-points that also service non-wLCG VOs that are not themselves implement acceptable identity vetting mechanisms.

Interoperation and infrastructure integration commitment

wLCG realises the importance of ensuring seamless interoperation with peer and leveraged infrastructures, the use of standard access mechanisms and interoperability at the level of the sites with other communities utilising the same services. Specifically, wLCG asserts that it shall not be necessary at the sites to deploy separate instances of the same service exclusively for wLCG purposes.

[17] urn:oid:1.2.840.113612.5.2.5.2 (being the technology-agnostic assurance elements of the MICS AP)
[18] https://www.igtf.net/ap/loa
[19] CEDAR is the generalized LoA identifier of which the Classic AP is the PKIX implementation

In current absence of proper software support, but in line with the long-term desire to support all IOTA accredited CAs, wLCG proposes the acceptance of a single, specific, PKI credential issuing authority ("CERN LHC IOTA CA"), that will in and by itself implement all the restrictions on VO eligibility for its subscribers (users), such that the combined authorization policy ("both LHC community and IOTA") is enforced already at the point of credential delivery. Having this policy enforced by the CA obviates the need at the sites to make the more complex combined decision in software, allowing them to accept specifically the "CERN LHC IOTA CA" as part of their standard trust fabric. By policy, the inclusion of this "CERN LHC IOTA CA" will be of no effect to any other communities or users, since such users will not have the possibility to obtain credentials from the "CERN LHC IOTA CA".

Remediation of collateral use of the CERN LHC IOTA CA outside the LHC context

It cannot be precluded that LHC users that are legitimately enrolled in an LHC VO will attempt to use their "CERN LHC IOTA" credential also in the context of other communities and VOs. This cannot technically be prevented. However, in such cases the CERN Computer Security Team will make available on request, and under the conditions detailed in the wLCG security policies, to any wLCG party such information as would have been contained in a MICS CERN CA certificate, based on VO and HR registration data, and the CERN Computer Security Team will support the wLCG participants involved with incident response based on the VO registration data contained in the LHC VO Management Services and relevant CERN HR data.

In addition, the CERN LHC IOTA CA may include the VO affiliation as part of the subject name of the certificate, permitting retroactive inspection of association based on accounting data.

In order to further limit risk, the availability of credentials from the CERN LHC IOTA CA, and the deployment use cases, shall be limited use cases that have been submitted, reviewed and approved explicitly by the wLCG management board.