Charter:

Device Level Security Mandate's Impact on Federated Access Working Group

Folder: 2025 Device Level Security Impact on Federation Working Group
Problem Statement: Problem Statement - Device-level Security in Federation
Status: draft

1. Overview

As research and education institutions increasingly rely on a diverse array of connected devices, ensuring robust device-level security has become a critical challenge. Many organizations struggle with securing devices at scale, managing endpoint security policies, and addressing emerging threats.

This working group seeks to assess the landscape of device-level security deployment across higher education, develop recommendations where feasible, and establish standard mechanisms to signal device-level security needs and enforcement between a relying party and an identity provider in a federated single sign-on (SSO) transaction. By bringing together security experts and stakeholders, this group will document current practices, identify gaps, and propose guidelines that promote consistency, scalability, and interoperability in securing devices across various environments.

2. Working Group Goals and Deliverables

The primary goal of the Device-Level Security Working Group is to develop practical guidance and standard signaling mechanisms for device security in federated identity transactions. Specific deliverables include:

- **Landscape Assessment:** Evaluating current device security deployment approaches across higher education.

- **Threat Analysis:** Identifying common security threats to institutionally managed and unmanaged devices, such as BYOD
- **Best Practices Document:** A detailed guide outlining effective device security strategies, including endpoint protection, secure configurations, monitoring, and compliance.
- **Policy Recommendations:** Guidelines for institutions to develop security policies tailored to different types of devices.
- **Federated Security Signaling Mechanisms:** Developing standard methods for identity providers and relying parties to communicate and enforce device-level security requirements within federated SSO transactions.
- **Implementation Guidance:** Practical recommendations for integrating device security solutions within existing IT and security infrastructures.
- **Preserving Privacy:** Develop recommendations on how to allow for BYOD privacy when evaluating device security posture

3. Scope

This working group will focus on:

- Assessing the landscape of device security deployments in research and education
- Developing standard mechanisms for signaling and enforcing device security needs in federated SSO
- Endpoint security for institutionally owned and personally managed devices
- Secure device configurations and management
- Network access controls and segmentation
- Security monitoring and incident response for endpoint devices
- Compliance and policy enforcement for device security

The group will not develop new security standards but will document best practices that align with existing cybersecurity frameworks and regulations.

4. Community and Stakeholders

The working group will engage stakeholders from:

- Research and education institutions
- IT security professionals
- Identity and access management professionals

- Network and endpoint security teams
- Policy and compliance officers
- Vendors and technology providers specializing in device security

5. Work Plan and Timeline

The working group will operate over a defined period, with the following proposed timeline:

- **Phase 1 (Months 1-3):** Assess current device security deployments and collect use cases.
- **Phase 2 (Months 4-6):** Conduct a threat analysis and draft initial best practices.
- **Phase 3 (Months 7-9):** Develop policy recommendations and federated security signaling mechanisms.
- **Phase 4 (Months 10-12):** Finalize documents and seek community feedback before publication.

6. Participation and Meetings

The working group is open to all interested parties. Regular virtual meetings will be held, with additional asynchronous collaboration through mailing lists and document-sharing platforms.

7. Coordination with Other Efforts

This working group will coordinate with relevant cybersecurity and identity management initiatives, such as REFEDS, InCommon, REN-ISAC, EDUCAUSE, and NIST guidelines. The group will ensure alignment with existing security frameworks and best practices in the field.

8. Leadership and Coordination

The working group will be chaired by individuals with experience in IT security and federated identity management. A facilitator will coordinate meetings, documentation, and community engagement.

9. Conclusion

The Device-Level Security Working Group aims to bridge the gap in endpoint security guidance by providing practical recommendations and developing standard mechanisms for signaling device security needs within federated SSO transactions. The outputs of this group will help institutions implement robust security practices and improve access control based on device security posture.

10. Terms

The following terms apply to all InCommon Technical Advisory Committee (TAC) Working Groups:

1. When a working group is agreed, the TAC Sponsor will place a call for participation in the InCommon community.
2. A chair, and optionally co-chairs, for the group is chosen from interested parties from the community.
3. Internet2 provides facilities for the working group, including meeting support, wiki space, and mailing lists.
4. An appropriate output from the group is produced. This is typically a working group report, proposed specifications and / or guidance documents.
5. When the Working Group is in agreement, the chair shares the outputs with the wider InCommon community with an open period for discussion and comment. This is typically a period of 4 weeks, but may be longer if appropriate.
6. After this period of time, TAC signs off on the work item. The InCommon Steering Committee may review, endorse, and/or approve the work item. Work is either written up as a formal white paper, left on the wiki but promoted as finished work or occasionally submitted as an Internet Draft.

11. References

TBD