Digital Imaging and Communications in Medicine (DICOM)

Whitepaper: DICOM supports compliance with

US Executive Order M-22-09

Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

*Prepared by:*

**DICOM Standards Committee, Working Group 14 - Security**

1300 N. 17th Street, Suite 900

Rosslyn, Virginia 22209 USA

Status: Working Draft for Comment

**Table of Contents**

Document History 4

Open Issues 4

Closed Issues 4

Summary 4

1 References 5

2 Identity management 5

2.1 MFA support requirements 5

2.2 Authorization controls 5

2.2.1 Role Based Access Control (RBAC) 5

2.2.2 Attribute Based Access Control (ABAC) 5

3 Device Inventory support 5

4 EDR Tools deployed and in use 5

5 DNS and Applications Communications 5

5.1 DNS 6

5.2 Applications Communications (DICOM) 6

6 Micro-segmentation 6

7 Audit logs 6

# Document History

|  |  |  |  |
| --- | --- | --- | --- |
| 12 Feb 2022 | 01 | Rjh | Initial draft |
| 23 May 2022 | 03 | Rjh | Review draft |
|  |  |  |  |

# Open Issues

|  |  |
| --- | --- |
| 1 | DICOM Question – Are the existing user identity negotiation capabilities sufficient? We can assume that the user identity interactions are out of scope for DICOM, but can we convey the results sufficiently? If so, what’s the note or informative section that we should write to explain how DICOM supports MFA. |
| 2 | DICOM Question – Aside from C-ECHO, is there anything else that DICOM has or should do to assist with device inventory support? For example, should C-ECHO also respond with the extended equipment information? DICOM Web has various capabilities descriptions, do these apply? Should they be extended? |

# Closed Issues

|  |  |
| --- | --- |
|  |  |
|  |  |

# Summary

The US Presidential Executive Order M-22-09 *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* 26 January, 2022specifies a variety of functional requirements. Some of these requirements apply to all applications and application communication used by the Federal government. This means that they will apply to DICOM compliant equipment used by the Federal government. There may be flow through requirements on vendors, contractors, lessors, etc. from the Federal government. The details of these requirements will depend upon decisions made by the relevant agencies.

The DICOM standard is an enabler for some of these requirements. Most of the requirements are process and feature requirements that apply to devices and healthcare providers.

The specific zero trust features the DICOM can enable are:

* Identity management
	+ MFA support requirements, including PIV (the US Government identity smart card) and Derived PIV, e.g., Web Authentication and FIDO 2
* Applications communication by TLS
* Audit logs

These DICOM capabilities are optional and configurable by products. If the product complies with the DICOM Conformance Claim specification (which most products do), the availability of these features is documented in a consistent manner and location by all vendors.

## Identity management

DICOM supports the exchange of user identity information, with the recommendation that this exchange take place over TLS protected links. This exchange can be

* username,
* username/password,
* Kerberos tickets (used by Active Directory),
* SAML Assertions (used by a variety of authentication systems including MFA systems),
* JWT Assertions (used by a variety of authentication systems including MFS systems).

DICOM does not specify any particular MFA systems or other authentication systems. It standardizes the exchange of authentication information between end points. Integration between specific authentication products and DICOM should be documented in the DICOM Conformance Claim.

## Device Inventory support

DICOM defines some very limited support for device inventory. For all DICOM devices there is a required ability to confirm that an endpoint address supports DICOM. DICOM connections can query and determine whether specific DICOM services are available.

These capabilities are useful for confirming inventory details, but not for discovering DICOM services or creating a device inventory.

## Applications Communications

DICOM defines support for link encryption and endpoint encryption using TLS. Specific capabilities are optional and may be configured by vendors and customers. DICOM has recommended profiles for TLS that correspond to US, European, and Japanese recommendations. These profiles correspond to current US TLS recommendations.

## Audit logs

DICOM defines a standard auditing format for events related to DICOM operations and activity. These are also extended and verified as part of the IHE process. The DICOM auditing covers some of the level 0 requirements of M-21-31 *Improving the Federal Government’s Investigative and Remediation Capabilities Related to Cybersecurity Incidents*.

##  References

*M-21-21 Improving the Federal Government’s Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, 27 August, 2021 <https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf>

*M-22-09 Moving the U.S. Government Toward Zero Trust Cybersecurity Principles,* 26 January, 2022[*https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf*](https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf)