Boeing SecureBadge Medium G3 Certificate Profiles

Description

Provides details about the CA's certificate and all certificates that the CA will issue.

Content Owner

BES PKI

All future revisions to this document shall be approved by the content owner prior to release.

Contents

Certificate Lifecycle

This table depicts each certificate described within this document and the certificates validity period in years. An Actual certificate's validity period may vary from standard (e.g., due to certificate renewal with a shorter validity period). The variance is not depicted in the certificate profile document. Deviating from the standard validity period requires OAA approval.

Certificate	Type	Validity Period	1	2	3	4	5	10	15	20
Boeing PCA G3	Root CA	20 Years								
Boeing Medium Assurance Hardware Issuing CA G3	Issuing CA	10 Years								
Boeing Medium Content Signer G2	Issued Certificate	10 Years								
Boeing Medium Qualified Subordinate	Qualified Subordination	7 Years								
Boeing Medium Enrollment Agent G2	Issued Certificate	5 Years								
Boeing Medium SecureBadge Identity G3	Issued Certificate	3 Years								
Boeing Medium SecureBadge Signature G3	Issued Certificate	3 Years								
Boeing Medium SecureBadge Encryption G3	Issued Certificate	3 Years								
Boeing Medium SecureBadge Card Authentication G3	Issued Certificate	3 Years								
Boeing Medium Key Recovery Agent G2	Issued Certificate	3 Years								
Boeing PCA G3 to CBCA G3	Cross Certificate	15 Months								
CA Exchange	Issued Certificate	7 Days								
Boeing MAH OCSP Response Signing	Issued Certificate	120 Days								

Object Identifiers (OIDs)

The following table summarizes the Certificate Policy object identifiers (OIDs) used by the certificates detailed within this document.

OID Number	Description
1.3.6.1.4.1.73.15.3	Boeing Public Key Infrastructure
1.3.6.1.4.1.73.15.3.1	Boeing Certificate Policies
1.3.6.1.4.1.73.15.3.1.11	Boeing Medium Assurance Software – SHA256
1.3.6.1.4.1.73.15.3.1.12	Boeing Medium Assurance Hardware – SHA256
1.3.6.1.4.1.73.15.3.1.15	Boeing Medium Assurance Hardware Card Auth – SHA256

Root Certificate Authority Profile(s)

Boeing PCA G3

Intended use .....Establishes the Boeing Medium Assurance Hardware Issuing CA G3 CA's authority to issue SHA-256 MAH SecureBadge certificates.

Business Rules.....Boeing does not publish the self-signed PCA certificate externally. External relying parties may refer to the contact in section 1.5.2 of the Medium Assurance Domain Certificate Policy published on the Boeing PKI Repository. The self-signed PCA certificate is made available internally via enterprise trust stores.

Authorized RAs.....N/A

Certificate Profile

Version	V3
Serial Number	Must be unique
Signature Algorithm	SHA256RSA
Signature Hash Algorithm	SHA256
Issuer	CN=Boeing PCA G3, OU=CertServers, O=Boeing, C=US
Validity Period	20 years
Subject	CN=Boeing PCA G3, OU=CertServers, O=Boeing, C=US
Public Key Algorithm	2048 bit RSA
Extended Key Usage	*No value specified*
CA Version	V0.0
Subject Key Identifier	critical=no, Octet String
Certificate Policies	All issuance policies
Certificate Template Name	*No value specified*
Authority Key Identifier	critical=no, Octet String
CRL Distribution Points	*No value specified*
Authority Information Access	*No value specified*
Key Usage	critical=yes, Digital Signature, Non-Repudiation, Certificate Signing, Off-line CRL Signing, CRL Signing (0xc6)
Basic Constraints	critical=yes, Subject Type=CA, Path Length Constraint=None

Boeing PCA G3 to CBCA G3

Intended use .....Establishes the CertiPath Bridge CA – G3 certified trust by Boeing.

Business Rules.....Boeing provisions internally the Boeing-issued-to-CertiPath cross certificate in the untrusted certificate store for proper chaining purposes.

Authorized RAs.....N/A

Certificate Profile

Version	V3
Serial Number	Must be unique
Signature Algorithm	SHA256RSA
Signature Hash Algorithm	SHA256
Issuer	CN=Boeing PCA G3, OU=CertServers, O=Boeing, C=US
Validity Period	15 months
Subject	CN=CertiPath Bridge CA – G3, OU=Certification Authorities, O=CertiPath, C=US
Public Key Algorithm	4096 bit RSA
Extended Key Usage	*No value specified*
CA Version	*No value specified*
Subject Key Identifier	critical=no, Octet String
Certificate Policies	critical=no, Policy Identifier=(1.3.6.1.4.1.73.15.3.1.11) Policy Identifier=(1.3.6.1.4.1.73.15.3.1.12)
Certificate Template Name	*No value specified*
Authority Key Identifier	critical=no, Octet String
CRL Distribution Points	critical=no, URL=http://crl.boeing.com/crl/Boeing%20PCA%20G3.crl
Authority Information Access	critical=no, URL=http://crl.boeing.com/crl/BoeingPCAG3.p7c
Key Usage	critical=yes, Certificate Signing, Off-line CRL Signing, CRL Signing (0x06)
Basic Constraints	critical=yes, Subject Type=CA, Path Length Constraint=None
InhibitAnyPolicy	critical=no, skipCerts=0
Name Constraints	critical=yes, Permitted=None, Excluded subtrees, RFC822 Name: boeing.com DNS Name: boeing.com Directory Address: O=Boeing, C=US
Policy Mapping	critical=no, (1.3.6.1.4.1.73.15.3.1.11)=(1.3.6.1.4.1.24019.1.1.1.1) (1.3.6.1.4.1.73.15.3.1.12)=(1.3.6.1.4.1.24019.1.1.1.2)

Boeing Medium Qualified Subordination

Intended use .....Identifies the qualified subordinate for the purposes of issuing cross certificates.

Business Rules.....*None specified*

Authorized RAs.....N/A

Certificate Profile

Version	V3
Serial Number	Must be unique
Signature Algorithm	SHA256RSA
Signature Hash Algorithm	SHA256
Issuer	CN=Boeing PCA G3, OU=CertServers, O=Boeing, C=US
Validity Period	7 years
Subject	CN=<first><last>
Public Key Algorithm	2048 bit RSA
Extended Key Usage	critical=no, Qualified Subordination (1.3.6.1.4.1.311.10.3.10)
Subject Key Identifier	critical=no, Octet String
Authority Key Identifier	critical=no, Octet String
CRL Distribution Points	critical=no, URL=http://crl.boeing.com/crl/Boeing%20PCA%20G3.crl
Authority Information Access	critical=no, Certification Authority Issuers: URL=http://ocsp.boeing.com:8080 Certification Authority Issuers: URL=http://crl.boeing.com/crl/BoeingPCAG3.p7c
Certificate Template	*No value specified*
Certificate Policies	*No value specified*
Application Policies	[1]Application Certificate Policy: Policy Identifier=Qualified Subordination
Key Usage	*No value specified*
Basic Constraints	critical=yes, Subject Type=End Entity, Path Length Constraint=None

Issuing Certificate Authority Profile(s)

Boeing Medium Assurance Hardware Issuing CA G3

Intended use .....Establishes the MAH CA's authority to issue MAH SecureBadges.

Authorized RAs.....MyID

Certificate Profile

Version	V3
Serial Number	Must be unique
Signature Algorithm	SHA256RSA
Signature Hash Algorithm	SHA256
Issuer	CN=Boeing PCA G3, OU=certservers, O=Boeing, C=US
Validity Period	10 years
Subject	CN=Boeing Medium Assurance Hardware Issuing CA G3, OU=CertServers, O=Boeing, C=US
Public Key Algorithm	2048 bit RSA
Extended Key Usage	*No value specified*
CA Version	V1.0
Subject Key Identifier	critical=no, Octet String
Certificate Policies	critical=no, Policy Identifier=(1.3.6.1.4.1.73.15.3.1.11) Policy Identifier=(1.3.6.1.4.1.73.15.3.1.12) Policy Identifier=(1.3.6.1.4.1.73.15.3.1.15)
Certificate Template Name	SubCA
Authority Key Identifier	critical=no, Octet String
CRL Distribution Points	critical=no, Certification Authority Issuers: URL=http://crl.boeing.com/crl/Boeing%20PCA%20G3.crl
Authority Information Access	critical=no,Certification Authority Issuers: URL=http://crl.boeing.com/crl/BoeingPCAG3.p7c
Key Usage	critical=yes, Digital Signature, Non-Repudiation, Certificate Signing, Off-line CRL Signing, CRL Signing (0xc6)

Basic Constraints	critical=yes, Subject Type=CA, Path Length Constraint=0

Issued Certificate Profile(s)

Boeing Medium SecureBadge Identity G3

Intended use .....Identifies an individual for Windows/application logon, connection to the BoeingNet wireless network, and authentication to WSSO and/or authorized external websites/applications.

Business Rules.....Base64 encoding of the certificate's public key published in the subject's directory entry in the people branch of EDS.

Authorized RAs.....MyID

Certificate Profile

Version	V3
Serial Number	Must be unique
Signature Algorithm	SHA256RSA
Signature Hash Algorithm	SHA256
Issuer	CN= Boeing Medium Assurance Hardware Issuing CA G3, OU=CertServers, O=Boeing, C=US
Validity Period	3 years
Subject	CN= <first>.<mi>.<last>.<bemsid>, OU=people, O=Boeing, C=US
Public Key Algorithm	2048 bit RSA
Extended Key Usage	critical=no, Client Authentication (1.3.6.1.5.5.7.3.2), Smart Card Logon (1.3.6.1.4.1.311.20.2.2), id-pkinit-KPClientAuth (1.3.6.1.5.2.3.4)
Subject Key Identifier	critical=no, Octet String
Authority Key Identifier	critical=no, Octet String
CRL Distribution Points	critical=no, URL=http://crl.boeing.com/crl/Boeing%20Medium%20Assurance%20Hardware%20Issuing%20CA%20G3.crl
Authority Information Access	critical=no, Certification Authority Issuers: URL=http://ocsp.boeing.com:8080 Certification Authority Issuers: URL=http://crl.boeing.com/crl/Boeing Medium Assurance Hardware Issuing CA G3.p7c
Certificate Template	critical=no,

	Template display name: Boeing Medium SecureBadge Identity G3 Object identifier: 1.3.6.1.4.1.311.21.8.9079547.13746898.10567832.14065279.6000620.73.9696245.11377414 Subject type: User Major version number: 100 Minor version number: 9
Certificate Policies	critical=no, Policy Identifier=(1.3.6.1.4.1.73.15.3.1.12)
Application Policies	critical=no, Client Authentication (1.3.6.1.5.5.7.3.2), Smart Card Logon (1.3.6.1.4.1.311.20.2.2), id-pkinit-KPClientAuth (1.3.6.1.5.2.3.4)
Subject Alternative Name	critical=no, Principal Name=<first>.<mi>.<last>@boeing.com URL= urn:uuid:<32 hex representing 128 bit GUID> (optional) others optional
Key Usage	critical=yes, Digital Signature (0x80)

Boeing Medium SecureBadge Signature G3

Intended use .....Identifies an individual for document signing. The certificate can be used to sign email messages.

Business Rules.....*None specified*

Authorized RAs.....MyID

Certificate Profile

Version	V3
Serial Number	Must be unique
Signature Algorithm	SHA256RSA
Signature Hash Algorithm	SHA256
Issuer	CN=Boeing Medium Assurance Hardware Issuing CA G3, OU=CertServers, O=Boeing, C=US
Validity Period	3 years
Subject	CN=<first>.<mi>.<last>.<bemsid>, OU=people, O=Boeing, C=US
Public Key Algorithm	2048 bit RSA
Extended Key Usage	critical=no, Document Signing (1.3.6.1.4.1.311.10.3.12), Secure Email (1.3.6.1.5.5.7.3.4), Adobe Authentic Document Trust (1.2.840.113583.1.1.5)
Subject Key Identifier	critical=no, Octet String
Authority Key Identifier	critical=no, Octet String
CRL Distribution Points	critical=no, URL=http://crl.boeing.com/crl/Boeing%20Medium%20Assurance%20Hardware%20Issuing%20CA%20G3.crl
Authority Information Access	critical=no, Certification Authority Issuers: URL=http:ocsp.boeing.com:8080 Certification Authority Issuers: URL=http://crl.boeing.com/crl/Boeing Medium Assurance Hardware Issuing CA G3.p7c
Certificate Template	critical=no, Template display name: Boeing Medium SecureBadge Signature G3 Object identifier: 1.3.6.1.4.1.311.21.8.9079547.13746898.10567832.14065279.6000620.73.11912736.1730175 Major version number: 100

	Minor version number: 8
Certificate Policies	critical=no, Policy Identifier=(1.3.6.1.4.1.73.15.3.1.12)
Application Policies	critical=no, Document Signing (1.3.6.1.4.1.311.10.3.12), Secure Email (1.3.6.1.5.5.7.3.4), Adobe Authentic Document Trust (1.2.840.113583.1.1.5)
Subject Alternative Name	critical=no, RFC822 Name=e-mail address, URL=urn:uuid:<32 hex representing 128 bit GUID> (optional) others optional
Key Usage	critical=yes, Digital Signature, Non-Repudiation (0xc0)

Boeing Medium SecureBadge Encryption G3

Intended use .....Identifies an individual for use with email encryption.

Business Rules.....*None specified*

Authorized RAs.....MyID

Certificate Profile

Version	V3
Serial Number	Must be unique
Signature Algorithm	SHA256RSA
Signature Hash Algorithm	SHA256
Issuer	CN=Boeing Medium Assurance Hardware Issuing CA G3, OU=CertServers, O=Boeing, C=US
Validity Period	3 years
Subject	CN=<first>.<mi>.<last>.<bemsid>, OU=people, O=Boeing, C=US
Public Key Algorithm	2048 bit RSA
Extended Key Usage	critical=no, Secure Email (1.3.6.1.5.5.7.3.4)
Subject Key Identifier	critical=no, Octet String
Authority Key Identifier	critical=no, Octet String
CRL Distribution Points	critical=no, URL=http://crl.boeing.com/crl/Boeing%20Medium%20Assurance%20Hardware%20Issuing%20CA%20G3.crl
Authority Information Access	critical=no, Certification Authority Issuers: URL=http:ocsp.boeing.com:8080 Certification Authority Issuers: URL=http://crl.boeing.com/crl/Boeing Medium Assurance Hardware Issuing CA G3.p7c
Certificate Template	critical=no, Template display name: Boeing Medium SecureBadge Encryption G3 Object identifier: 1.3.6.1.4.1.311.21.8.9079547.13746898.10567832.14065279.6000620.73.15524037.2658325 Major version number: 100 Minor version number: 33

Certificate Policies	critical=no, Policy Identifier=(1.3.6.1.4.1.73.15.3.1.12)
Application Policies	critical=no, Policy Identifier=Secure Email (1.3.6.1.5.5.7.3.4)
Subject Alternative Name	critical=no, RFC822 e-mail address, URL=urn:uuid:<32 hex representing 128 bit GUID> (optional) others optional
Key Usage	critical=yes, Key Encipherment (0x20)

Boeing Medium SecureBadge Card Authentication G3

Intended use .....Identifies a particular MAH SecureBadge and specifies the mandatory asymmetric Card Authentication Key (CAK) as a private key that is intended be used to support physical access applications (e.g. may contain biometrics for door access) or other use cases needing specific attributes in the certificate.

Business Rules.....Use of this certificate is not permitted without proper PKI Governing Authorities' approval.

Authorized RAs.....MyID

Certificate Profile

Version	V3
Serial Number	Must be unique
Signature Algorithm	SHA256RSA
Signature Hash Algorithm	SHA256
Issuer	CN=Boeing Medium Assurance Hardware Issuing CA G3, OU=CertServers, O=Boeing, C=US
Validity Period	3 years
Subject	OU=people, O=Boeing, C=US
Public Key Algorithm	2048 bit RSA
Extended Key Usage	critical=yes, id-PIV-cardAuth (2.16.840.1.101.3.6.8)
Subject Key Identifier	critical=no, Octet String
Authority Key Identifier	critical=no, Octet String
CRL Distribution Points	critical=no, URL=http://crl.boeing.com/crl/Boeing%20Medium%20Assurance%20Hardware%20Issuing%20CA%20G3.crl
Authority Information Access	critical=no, Certification Authority Issuers: URL=http://ocsp.boeing.com:8080 Certification Authority Issuers: URL=http://crl.boeing.com/crl/Boeing Medium Assurance Hardware Issuing CA G3.p7c
Certificate Template	critical=no, Template display name: Boeing Medium SecureBadge Card Authentication G3

	Object identifier: 1.3.6.1.4.1.311.21.8.9079547.13746898.10567832.14065279.6000620.73.9306309.5754857 Major version number: 100 Minor version number: 33
Certificate Policies	critical=no, Policy Identifier=(1.3.6.1.4.1.73.15.3.1.15)
Application Policies	critical=yes, id-PIV-cardAuth (2.16.840.1.101.3.6.8)
Subject Alternative Name	critical=no, URL=urn:uuid:<32 hex representing 128 bit GUID> (optional) others optional
Key Usage	critical=yes, Digital Signature (0x80)

Boeing Medium Enrollment Agent G2

Intended use .....Identifies the MyID service account for requesting MAH SecureBadge certificates.

Business Rules.....The application policy is suppressed in any leaf certificates (per the CertiPath 2023 interoperability test).

Authorized RAs.....N/A

Certificate Profile

Version	V3
Serial Number	Must be unique
Signature Algorithm	SHA256RSA
Signature Hash Algorithm	SHA256
Issuer	CN=Boeing Medium Assurance Hardware Issuing CA G3, OU=CertServers, O=Boeing, C=US
Validity Period	5 years
Subject	CN=MyID Service, OU=Service Accounts, OU=BADGE, DC=badge, DC=pki, DC=boeing, DC=net
Public Key Algorithm	2048 bit RSA
Extended Key Usage	critical=no, Enrollment Agent (1.3.6.1.4.1.311.20.2.1)
Subject Key Identifier	critical=no, Octet String
Authority Key Identifier	critical=no, Octet String
CRL Distribution Points	critical=no, URL=http://crl.boeing.com/crl/Boeing%20Medium%20Assurance%20Hardware%20Issuing%20CA%20G3.crl
Authority Information Access	critical=no, Certification Authority Issuers: URL=http://ocsp.boeing.com:8080 Certification Authority Issuers: URL=http://crl.boeing.com/crl/Boeing%20Medium%20Assurance%20Hardware%20Issuing%20CA%20G3.p7c
Certificate Template	critical=no, Template display name: Boeing Medium Enrollment Agent G2 Object identifier: 1.3.6.1.4.1.311.21.8.9079547.13746898.10567832.14065279.6000620.73.14817356.15775187

	Major version number: 100 Minor version number: 23
Certificate Policies	*No value specified*
Application Policy	critical=no, Certificate Request Agent (1.3.6.1.4.1.311.20.2.1)
Key Usage	critical=yes, Digital Signature (0x80)

Boeing Medium Content Signer G2

Intended use .....Identifies the MyID service account to sign PIV content on the MAH SecureBadge.

Business Rules.....*None specified*

Authorized RAs.....N/A

Certificate Profile

Version	V3
Serial Number	Must be unique
Signature Algorithm	SHA256RSA
Signature Hash Algorithm	SHA256
Issuer	CN=Boeing Medium Assurance Hardware Issuing CA G3, OU=CertServers, O=Boeing, C=US
Validity Period	10 years
Subject	CN=MAHPIVContentSigner
Public Key Algorithm	2048 bit RSA
Extended Key Usage	critical=yes, id-fpki-pivi-content-signing (2.16.840.1.101.3.8.7)
Subject Key Identifier	critical=no, Octet String
Authority Key Identifier	critical=no, Octet String
CRL Distribution Points	critical=no, URL=http://crl.boeing.com/crl/Boeing%20Medium%20Assurance%20Hardware%20Issuing%20CA%20G3.crl
Authority Information Access	critical=no, Certification Authority Issuers: Certification Authority Issuers: URL=http://crl.boeing.com/crl/Boeing%20Medium%20Assurance%20Hardware%20Issuing%20CA%20G3.p7c URL=http://ocsp.boeing.com:8080
Certificate Template	critical=no, Template display name: Boeing Medium Content Signer G2 Object identifier: 1.3.6.1.4.1.311.21.8.9079547.13746898.10567832.14065279.6000620.73.8039199.3126967 Major version number: 100

	Minor version number: 30
Certificate Policies	*No value specified*
Application Policies	critical=yes, id-fpki-pivi-content-signing (2.16.840.1.101.3.8.7)
Key Usage	critical=yes, Digital Signature (0x80)

Boeing Medium Key Recovery Agent G2

Intended use .....Identifies the MyID service account as a key recovery agent.

Business Rules.....The application policy is suppressed in any leaf certificates (per the CertiPath 2023 interoperability test).

Authorized RAs.....N/A

Certificate Profile

Version	V3
Serial Number	Must be unique
Signature Algorithm	SHA256RSA
Signature Hash Algorithm	SHA256
Issuer	CN=Boeing Medium Assurance Hardware Issuing CA G3, OU=CertServers, O=Boeing, C=US
Validity Period	3 years
Subject	CN=MAHKeyRecoveryAgent
Public Key Algorithm	2048 bit RSA
Extended Key Usage	critical=no, Key Recovery Agent (1.3.6.1.4.1.311.21.6)
Subject Key Identifier	critical=no, Octet String
Authority Key Identifier	critical=no, Octet String
CRL Distribution Points	critical=no, URL=http://crl.boeing.com/crl/Boeing%20Medium%20Assurance%20Hardware%20Issuing%20CA%20G3.crl
Authority Information Access	critical=no, Certification Authority Issuers: URL=http://ocsp.boeing.com:8080 Certification Authority Issuers: URL=http://crl.boeing.com/crl/Boeing%20Medium%20Assurance%20Hardware%20Issuing%20CA%20G3.p7c
Certificate Template	critical=no, Template display name: Boeing Medium Key Recovery Agent G2 Object identifier: 1.3.6.1.4.1.311.21.8.9079547.13746898.10567832.14065279.6000620.73.12201302.2241609 Major version number: 100

	Minor version number: 20
Certificate Policies	*No value specified*
Application Policies	critical=no, Key Recovery Agent (1.3.6.1.4.1.311.21.6)
Key Usage	critical=yes, Key Encipherment (0x20)

CA Exchange

Intended use .....Identifies the MAH SecureBadge CA for the purposes of key archival.

Business Rules.....*None specified*

Authorized RAs.....N/A

Certificate Profile

Version	V3
Serial Number	Must be unique
Signature Algorithm	SHA256RSA
Signature Hash Algorithm	SHA256
Issuer	CN=Boeing Medium Assurance Hardware Issuing CA G3, OU=CertServers, O=Boeing, C=US
Validity Period	1 Year
Subject	CN=Boeing Medium Assurance Hardware Issuing CA G3-Xchg, OU=CertServers, O=Boeing, C=US
Public Key Algorithm	2048 bit RSA
Extended Key Usage	critical=no, Private Key Archival (1.3.6.1.4.1.311.21.5)
Subject Key Identifier	critical=no, Octet String
Authority Key Identifier	critical=no, Octet String
CRL Distribution Points	critical=no, URL=http://crl.boeing.com/crl/Boeing%20Medium%20Assurance%20Hardware%20Issuing%20CA%20G3.crl
Authority Information Access	critical=no, Certification Authority Issuers: URL=http://ocsp.boeing.com:8080 Certification Authority Issuers: URL=http://crl.boeing.com/crl/Boeing Medium Assurance Hardware Issuing CA G3.p7c
Certificate Template	critical=no, Template display name: CA Exchange Object identifier: 1.3.6.1.4.1.311.21.8.9079547.13746898.10567832.14065279.6000620.73.1.26 Subject type: Computer Major version number: 106

	Minor version number: 6
Certificate Policies	critical=no, Policy Identifier=(1.3.6.1.4.1.73.15.3.1.11) Policy Identifier=(1.3.6.1.4.1.73.15.3.1.12) Policy Identifier=(1.3.6.1.4.1.73.15.3.1.15)
Application Policies	critical=no, Policy Identifier=Private Key Archival
Subject Alternative Name	*No value specified*
Key Usage	critical=yes, Key Encipherment (0x20)

Boeing MAH OCSP Response Signing

Intended use .....OCSP Response Signing.

Business Rules.....All use cases must be approved by PKI Governing Authorities. The application policy is suppressed in any leaf certificates (per the CertiPath 2023 interoperability test).

Authorized RAs.....N/A

Certificate Profile

Version	V3
Serial Number	Must be unique
Signature Algorithm	sha256RSA (1.2.840.113549.1.1.11)
Signature Hash Algorithm	SHA256
Issuer	CN=Boeing Medium Assurance Hardware Issuing CA G3, OU=CertServers, O=Boeing, C=US
Validity Period	120 days
Subject	CN=<MAH_02_Month_Year of certificate issuance>, OU=servers, O=Boeing, C=US
Public Key Algorithm	2048 bit RSA
Authority Key Identifier	critical=no, Octet String
Certificate Template	Template display name: Boeing MAH OCSP Response Signing Object identifier: 1.3.6.1.4.1.311.21.8.9079547.13746898.10567832.14065279.6000620.73.16613077.15685628 Subject type: Computer Major version number: 100 Minor version number: 25
Subject Key Identifier	critical=no, Octet String
Key Usage	critical=yes, Digital Signature (0x80)
Extended Key Usage	critical=yes, OCSP Signing (1.3.6.1.5.5.7.3.9)
Certificate Policies	critical=no, Policy Identifier=(1.3.6.1.4.1.73.15.3.1.12) Policy Identifier=(1.3.6.1.4.1.73.15.3.1.15)
OCSP No Revocation Checking	critical=no, 05 00
Application Policies	OCSP Signing

Boeing MAH OCSP Response Signing Format

Field	Value
Response Status	As specified in RFC 6960
Response Type	Basic OCSP Response (1.3.6.1.5.5.7.48.1.1)
Version	V3
Responder ID	KeyHash as specified in RFC6960 (SHA-1 hash of the BIT STRING subjectPublicKey excluding the tag, length, and number of unused bits in the responder's certificate)
Produced At	Generalized Time
List of Responses	Each response will contain certificate id; certificate status, thisUpdate, nextUpdate
Responder Signature	sha256 WithRSAEncryption (1.2.840.113549.1.1.11)
Certificates	Applicable OCSP Responder certificates
Response Extension	Value
Nonce	critical=no, Value in the nonce field of request
Response Entry Extension	Value

Revision Record

Document Type	Original Release Date	Version/Revision
Artifact	5/17/2016	1.8

Changes in this version

- Initial version
- 6/13/17 - v1.1 Added SCA and Template information
- 9/5/17 – v1.2 Updated CA name references, version and additional updates from Key Generation
- 1/11/2018 – v1.3 Updated Template versions
- 4/1/2018 – v1.4 Update names for OIDs and revision due to CertiPath Interoperability report (OID and AIA changes)
- 5/17/2018 added proper descriptions to OIDs in the eku attribute; in the AIA attribute changed https to http in the P7C URL due to CA publishing limitation
- 7/19/2018 - Validity Period changed on CA Exchange, Content Signer and Enrollment agent templates to match Template
- 4/17/2020 – In the Boeing PCA G3 to CBCA G2 cert: Updated CertiPath CA Name to current CA Name and corrected Inhibit Any Policy name to InhibitAnyPolicy; in the Boeing Medium Enrollment Agent G2: moved Basic Constraints to standard location and added correct definitions; Changed Boeing Medium CA Exchange G2 to reflect default template used and it's CN name in the profile to what was is in the template "Boeing Medium Assurance Hardware Issuing CA G3-Xchg"; modified AIA to point to the existing URL's in the Certificates (.crt, ldap, .cer, and .p7c) where applicable; Standardized Certificate Policies attribute formatting in applicable certificates; Changed CA Exchange certificate to No Value Specified; Medium Enrollment Agent cert version changed from V2 to V3
- 4/30/2020 - Added "Boeing OCSP Response Signing" Template
- 5/28/2020 – Removed the LDAP URL from AIA and CDP in the CBCA cert profile
- 6/15/2020 – changed the validity period of the Boeing PCA G3 to CBCA G3 to 13 months
- 7/28/2020 – changed the "Boeing OCSP Response Signing" profile validity period to 45 days and added the response signing format
- 8/18/2020 - Modified the AIA to remove .crt and .cer and moved the .p7c to the top in all except the OCSP response Signing, CA exchange, Key Recovery, content signer, and Enrollment agent.
- 5/25/2021 - Modified intended use and business rules to reflect accurate description for Boeing Medium SecureBadge Identity G2, Boeing Medium SecureBadge Card Authentication G2, and Boeing OCSP Response Signing.
- 6/1/2021 – Updated O=Boeing, C=US for proper capitalization. Updated OU to reflect actual capitalization in certificates (OU:CertServers, OU:people, and OU:securebadge). In the Certificate Lifecycle chart, we corrected the name of the certificate (CA Exchange).
- 9/22/2021 - Modified the SecureBadge Signature to remove erroneous additional "name" information that was only in the certificate profile document, in addition to other general formatting corrections.
- 12/20/2021 – Removed CDP/AIA LDAP value from certificates (effective on renewals) (document only); updated Minor Version Number according to templates (document

only); Updated Application policies to replace No value specified with the current policies applied for: Boeing Medium SecureBadge Signature G2, Boeing Medium SecureBadge Encryption G2, Boeing Medium SecureBadge Card Authentication G2, Boeing Medium Enrollment Agent G2, Boeing Medium Content Signer G2, and Boeing Medium Key Recovery Agent G2 certificate profiles; removed extended key usage value: id-kp-emailProtection for Boeing Medium SecureBadge Signature G2 and Boeing Medium SecureBadge Encryption G2 certificate profile (document only); Updated template name from Boeing Medium CA Exchange G2 to CA Exchange and added certificate policy OIDs for CA Exchange template (document only); updated subject alternative name value from principle name (first.m.last) to Boeing email address of the recipient (document only); updated the name of the MAH OCSP Response Signing template and added certificate policies, updated the subject to match what is in the certificate, in the subject updated the format for the Common Name (CN), corrected OU from <servers> to servers, and updated OCSP No Revocation Checking to actual value provided by CSA (document only).

- 04/5/2022 – Removed CDP/AIA LDAP value from *all* remaining certificates (effective on renewals); corrected AIA value so OCSP address is displayed first, followed by the .p7c certificate address; and added Business Rules to PCA and Boeing cross certificate issued to CertiPath certificate profiles.
- 07/12/2022 – Updated validity period on Certificate Lifecycle table for Boeing Medium Key Recovery Agent G2, Boeing Medium Content Signer G2 and Boeing Medium Enrollment Agent G2 to match actual dates per profiles.
- 12/01/2022 – Updated validity period on the Boeing MAH OCSP Response Signing template from 45 days to 120 days and corrected the template name on the Certificate Lifecycle table.
- 8/09/2023 – Updated template names to G3 and updated the Certificate Template information.
- 8/26/2023 - Updated critical template names to G2 and updated the Certificate Template information.
- 6/12/2024 - The SCA certificate was renewed with a validity period change from 10 years to 6 years and 6 months on 06-12-2024 and this certificate profile document updated on 9/18/2024 to reflect the new validity period.
- 8/19/2024 - Updated from 13 months to 15 months and this certificate profile document updated 10/16/2024 to reflect this change.
- 10/24/2024 – Updated the paragraph under the Certificate Lifecycle heading and updated the validity period scale from 6 years and 6 months back to 10 years in accordance to Patty McClendon's email request.
- 7/10/2025 - Edits to the profile document as discovered from the Richter audit 2025. Update the CBCA to have a key length of 4096. Changed the CA Version of the Boeing Medium Assurance Hardware Issuing CA G3 to v1.0. Removed the Certification Authority Issuers of the OCSP from the Boeing Medium Assurance Hardware Issuing CA G3. Removed the Subject Type: User from the Boeing Medium SecureBadge Signature G3, Boeing Medium SecureBadge Encryption G3, Boeing Medium SecureBadge Card Authentication G3, Boeing Medium Content Signer G2, and Boeing Medium Enrollment Agent G2. Added the business rule note Use of this certificate is not permitted without proper PKI Governing Authorities' approval to the Boeing Medium Enrollment Agent G2, Boeing Medium Key Recovery Agent G2, Boeing Medium SecureBadge Card Authentication G3, and Boeing MAH OCSP Response Signing. Removed the Subject Type: Key Recovery from the Boeing Medium Key Recovery Agent G2. Removed the SMIME Capabilities from the Boeing Medium

Key Recovery Agent G2. Changed the certificate. Changed the Certificate Profile Version from 2 to 3 on Boeing Medium Key Recovery Agent G2 and Boeing Medium Content Signer G2. Removed the Basic Constraint from the Boeing Medium Enrollment Agent G2. Changed the Subject OU from securebadge to people in the Boeing Medium securebadge Card Authentication G3. This needs to be changed back to securebadge when the certificate is renewed. Updated the Table of Contents.

Author and Contributors

Author: Mark A Jupiter

Contributors: Patricia A. McClendon

Beverly J. Starks

Hamad A. Chawdhry

Colin McLeod

Signature for Release

Approval:	Signature on File	IS PKI	10/16/2024
	Patricia A. McClendon	Organization	Date