

Updating server certificates to improve end-user security and client user experience

Avaya Communicator 2.0
September 2014
Issue 1.1

© 2014 Avaya Inc.
All Rights Reserved.

Notice
While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

For full support information, see the complete documents, Avaya Support Notices for Software Documentation, document number 03-600758 and Avaya Support Notices for Hardware Documentation, document number 03-600759.

To locate this document on our Web site, go to www.avaya.com/support and search for the document number in the search box.

Documentation disclaimer
Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer
Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Warranty
Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product, while under warranty, is available through the following Web site: www.avaya.com/support.

Copyright
Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Avaya support
Avaya provides a telephone number for you to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: www.avaya.com/support.

Trademarks
Avaya and Avaya Aura are trademarks of Avaya Inc, registered in the United States and other countries. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the U.S. and/or other countries. Apple, Mac, and Mac OS X are trademarks of Apple Inc, registered in the U.S. and other countries. iOS is a trademark of Cisco Inc, used by Apple under license. Android is a trademark of Google Inc.

Contents

Background **2**
What are certificates? 2
Changes in the new generation of Avaya Communicator clients 2
Why is this happening? 3
What services are affected? 3

How to simplify your network **4**
Step 1 - Network Survey 5
Step 2 - Site Evaluation 6
Step 3 - Deployment 6

CA certificate distribution for Avaya client applications **7**
Windows 7
Mac OS X 7
iOS 8
Android 8
Avaya desk phones 8

Certificate reference **9**
Web service (server) certificates 10
SIP server certificates 11
XMPP server certificates 12
LDAP server certificates 13
"Generic TLS" server certificates - anything else 14

Sample server identity certificate **15**

Choosing a certificate vendor **16**

Troubleshooting certificate problems **17**
"The security certificate required for <...> is not installed" 17
"The security certificate required for <...> has expired" 17
"There is a <...> security certificate problem" 17

References **18**
Avaya product documentation 18
External standards 18

Summary

The new generation of Avaya Communicator clients will require servers to have certificates issued by a trusted certificate authority (CA) in order for the client to establish a secure connection. Administrators will have to review their networks to determine the certificates in use and decide whether to distribute CA certificates to end-user devices, to replace server certificates, or both. This document aims to provide administrators with the information and tools necessary to make this decision with minimal service disruption and end-user impact.

Administrators who choose to deploy server certificates issued by well-known vendors will avoid the potential complexity, errors, and support costs involved in alternative solutions.

Background

What are certificates?

Like passports or other physical forms of identification, certificates are an assertion of identity, issued and signed by an entity known as a certificate authority. Like their physical counterparts, certificates may be trusted or untrusted based on the relationship that the verifier has with the issuer. If the issuer is known to and trusted by the verifier, then the identity of the certificate bearer can be similarly trusted. If the issuer is not known and trusted, then the certificate cannot be trusted either.



As assertions of identity, certificates are used to establish trust and secured communications between entities on a network. When a client connects to a server, the client first asks the server to provide a certificate proving the server's identity. If the server is able to produce a certificate that the client trusts, then the client will allow the connection to proceed. The server may also ask the client to produce a certificate and perform validation of its own.

Digital certificates use public key cryptography, which relies on pairs of keys known as the private key and the public key. This pair of keys can be used to exchange and verify messages securely. As long as the private key remains secret, the system has a known level of security. However, if the private key is compromised, an attacker can potentially use the compromised private key to impersonate the target subject or potentially even decrypt previously-recorded traffic.

Most systems have additional measures in place to reduce the risk of compromised private keys, such as verifying that the certificate has not expired, that the content of the certificate matches some known attribute of the bearer, or using a revocation mechanism to invalidate certificates. As well, much like a person checking that the photo on a passport matches the appearance of the person carrying it, validators will typically also check that the certificate identity matches the host name being accessed.

Security and trust are established by creating a “chain of trust” from a certificate back to a known certificate issuer (“certificate authority”). There are many well-known certificate authorities (CAs) that have established relationships with operating system and device vendors in order to act as “trusted root CAs”. Each CA has its own identity certificate (a “CA certificate”) which is used as a “trust anchor”; if a certificate can be traced back to one of these trust anchor certificates and passes all of the other validity checks, then it can be used to establish a secure connection and the identity of the bearer. Many organizations have their own in-house CA whose certificate they distribute as an additional trust anchor. Avaya also created a private CA that issued default product certificates for demonstrations, lab purposes, and use in isolated private networks.

Changes in the new generation of Avaya Communicator clients

The new generation of Avaya Communicator clients will require servers to have certificates issued by a trusted certificate authority in order for the client to establish a secure connection. These clients will no longer trust demonstration certificates issued by the Avaya SIP Product Certificate Authority by default.

Why is this happening?

As with other forms of identification, certificate technology has progressed over the years. Current standards mandate using newer algorithms than are in place in the default certificates that Avaya has shipped with Avaya Aura systems for demonstration, lab, and isolated private network use, so use of these default certificates has now been deprecated and trust of the Avaya SIP Product Certificate Authority has been removed from new clients. Avaya's recommendation is that customers upgrade their servers to use certificates generated to the current United States National Institute of Standards and Technology (NIST) standards for information systems security. Detailed information for doing this upgrade is available in the product documentation.

The default certificates shipped with Avaya Aura Session Manager were intended for lab and demonstration use only. Up to now, clients have included support for these default certificates to facilitate lab testing. Removing support for these default certificates from the clients allows customers with higher security needs to implement a strategy using current best practices.

What services are affected?

All communications between the client and the servers in the Avaya Aura environment are secured using a technology called Transport Layer Security (TLS, a newer version of SSL that you may be familiar with). In TLS, servers are configured with an identity certificate issued by a certificate authority. When clients connect to servers, the server presents its identity certificate for the client to validate. The client checks whether the server identity certificate was issued by a certificate authority that the client trusts (among other items). If everything checks out, then the client proceeds and a secure connection is established.

In Figure 1 below, the color coding of each element reflects the issuing certificate authority for certificates presented by that element (see the legend for details). Elements which may have certificates from multiple authorities are shown using a gradient fill.

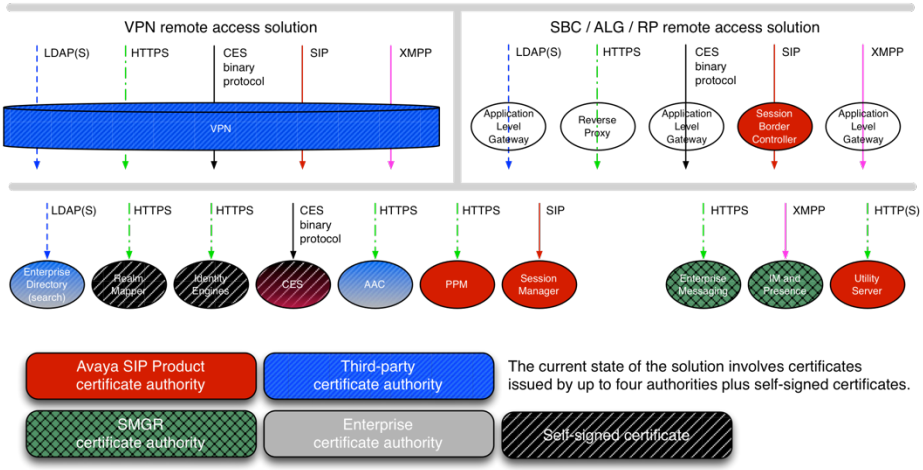

Figure 1 - Default certificates in the historical network infrastructure

Customers who have deployed the Avaya Unified Communications solution over time may have a very complex set of certificates and may require the installation of up to four CA certificates on client devices as well as replacing the default certificate on the Avaya one-X Client Enablement Services server. The Avaya Aura team is working to simplify this situation; new installations will use the Avaya Aura System Manager certificate authority where possible and eliminate use of the Avaya SIP Product certificate authority entirely.

How to simplify your network

Installing certificates issued by your enterprise certificate infrastructure or by a well-known certificate vendor will simplify your network and reduce the amount of work required for your users to start using the new Avaya clients. If you use a well-known certificate vendor that is already trusted by the end-user client devices, there is no need to deploy certificates to those devices at all. If you have an enterprise certificate infrastructure, you may need to make the CA certificate available to end users so that they can install it on their client device and provide instructions for them to do so.

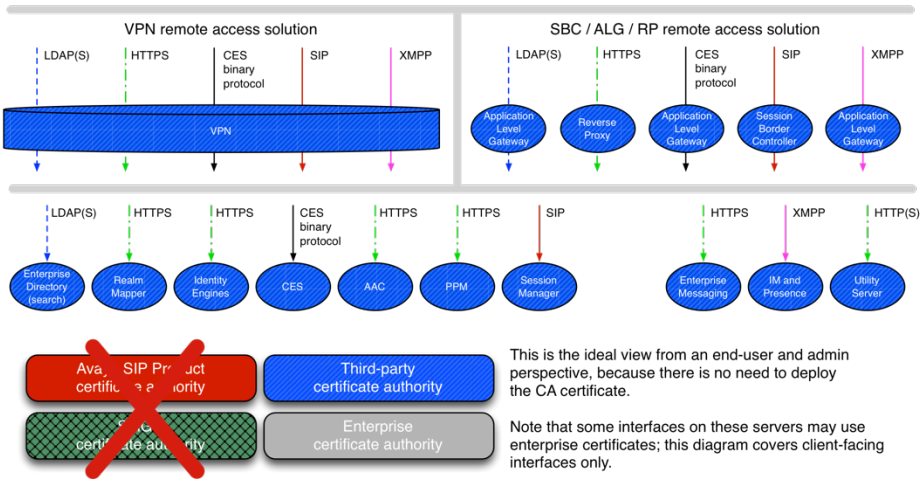

Figure 2 - Improved certificate architecture

The diagram above shows the primary recommendation, which is to use a well-known trusted third-party certificate authority for all client-facing interfaces in production. Following this recommendation will ensure the smoothest experience for end users in a production environment, as you will not need to distribute the CA certificate to devices. If you are running a non-production test environment or configuring non-client-facing interfaces (e.g. management interfaces or other internal communications links) you may choose to use certificates issued by your own enterprise certificate infrastructure or by the Avaya Aura System Manager CA. Because these interfaces are internal and do not involve distributing CA certificates to a large number of end devices, the additional complexity of using multiple CAs may be offset by the reduced cost.

Step 1 - Network Survey

Do a survey of all of the affected network elements and their interconnections. Focus on elements that face the clients and the external network:

- Avaya Aura Session Manager (including PPM)
- Avaya Session Border Controller for Enterprise
- Avaya Aura Conferencing (including web conferencing and document servers)
- Avaya Identity Engines (including Realm Mapper service)
- Avaya Client Enablement Services
- Avaya Multimedia Messaging
- Avaya Presence Server
- the Utility Server
- your enterprise directory server

You may also have additional third-party network elements participating in your network. Identify the interconnections between these elements and the rest of the network. As part of this survey, capture the software release number of each network element, including all of the clients and phone sets.

In your network survey, make note of all certificates used. Many network elements will have more than one certificate, and each certificate may have slightly different characteristics depending on the type of service. See Certificate reference on page 9 for a detailed description of the required attributes for each type of certificate.

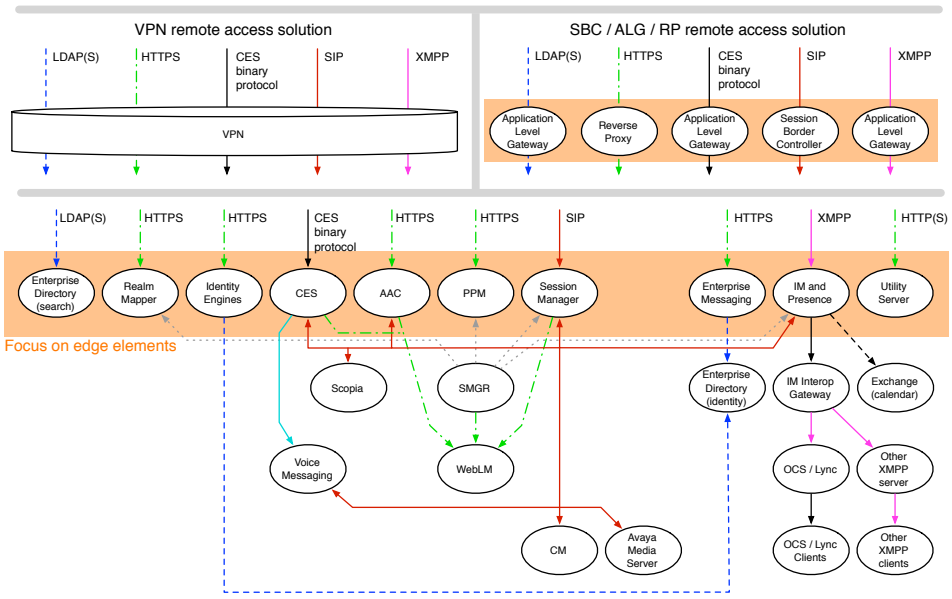

Figure 3 - Sample network diagram

Step 2 - Site Evaluation

Identify any elements of the network that need to be upgraded to support your new certificates. Some older versions of server software does not support replacing certificates. If you are using certificates of any length with SHA-2 digests, you should ensure you upgrade to a software release that supports SHA-2. Consult the product documentation for each of the elements in your network, including client applications and desk phones, to determine whether the installed software release supports the certificates you plan to install.

It is important to note that you need to validate that *both ends* of each communication link support the certificates you plan to install. For example, if you install a SHA-2 identity certificate on the Avaya Aura Session Manager "Security Module SIP" service, then all of the network elements which connect directly to the Avaya Aura Session Manager (in the diagram above: Avaya Aura Communication Manager, Avaya Media Server, Avaya Messaging Server, Avaya Client Enablement Services, Avaya Aura Conferencing, Scopia, Avaya Presence Server, all SIP desk phones, and all SIP soft clients) must support SHA-2.

Step 3 - Deployment

Deploy CA certificates throughout your network for the new CA

The first step is to ensure that the certificate authority (CA) issuing your identity certificates is trusted throughout your network. To do this, install the CA certificate into the trust stores on all of the network elements, including devices running client applications and desk phones. Instructions for updating the trust stores on each network element are detailed in the product documentation for each network element.

> *If you have elected to use a well-known trusted third-party certificate authority that is already supported by the devices running client applications, you will not need to deploy the CA certificate to these devices. However, you may still need to deploy the CA certificate to the servers and desk phones in your network.*
>
> *Note: Many network elements have multiple trust stores. Ensure that you install the new CA certificate(s) in all of the required trust stores.*

Deploy new server certificates

We recommend that updates start at the "periphery" of the network and move towards the core elements. When planning your update, identify the network elements with the fewest incoming links and start there. On each server, install the new server identity certificate and verify that all connections to the server are functioning properly. Instructions for updating the server identity certificate on each network element are detailed in the product documentation for each network element.

> *Note: Each server may have multiple service interfaces. Ensure that you install the appropriate new server certificates for each service interface.*

Remove support for the old CA certificate from your network

As a final step, once you have validated that your updates are complete and all elements are using certificates from your new certificate authority, you should remove trust for the old certificate authority. Instructions for updating the trust stores on each network element including the desk phones are detailed in the product documentation for each element.

> *Caution: Do not remove support for the old CA certificate from your network until the new CA certificate has been successfully installed and tested. Removing the old CA certificate prematurely can result in service outages.*

CA certificate distribution for Avaya client applications

Avaya client applications run on modern operating systems that have pre-configured trust for established certificate vendors; if you obtain certificates from one of these established vendors and install them on your servers, then you will not need to distribute CA certificates to your client computers and devices.

However, if your network is using certificates issued by the Avaya SIP Product certificate authority, Avaya Aura System Manager, an enterprise certificate authority, or a third-party certificate authority that is not well-known, you will need to ensure that the certificate authority (or authorities) that issued your server certificates is trusted by the client devices. To do that, you will need to distribute the CA certificates to the client devices and ensure that they are installed.

In general, there is a centralized mechanism for distributing CA certificates to managed devices and a separate mechanism for distributing certificates to unmanaged devices. Distributing CA certificates to unmanaged devices usually involves making them available on an internal website, sending them via email, or providing them on a portable storage device.

Installing certificates is a relatively streamlined process on all platforms; each provides a certificate import “wizard” experience. However, users do occasionally make mistakes or run into problems, so avoiding the need to install certificates on end-user devices is recommended.

Windows

For PCs running Windows, the preferred mechanism for deploying CA certificates to managed PCs is through Group Policy Objects. Refer to the Microsoft TechNet documentation for instructions on how to use policy to distribute and install certificates on managed PCs.

For unmanaged PCs, unless you use a well-known certificate vendor that is already trusted by the PC, your users will need to install CA certificates themselves. You will need to make the CA certificates available to users and give them instructions for installing these certificates into the **Trusted Root Certification Authorities** trust store on their PC. Refer to the Microsoft TechNet documentation for instructions on how to manually install certificates into the **Trusted Root Certification Authorities** trust store on the PC.

> *The Windows certificate installation wizard does not always install CA certificates into the correct trust store. You should advise users to manually select the **Trusted Root Certification Authorities** trust store when installing CA certificates.*

Mac OS X

For devices running Mac OS X, you can use Apple Remote Desktop or Profile Manager to deploy trusted CA certificates to managed computers. Refer to Apple support documentation for instructions on using Apple Remote Desktop or Profile Manager to distribute and install certificates on managed computers.

For unmanaged computers, unless you use a well-known certificate vendor that is already trusted by the computer, your users will need to install CA certificates themselves. You will need to make the CA certificates available to users and give them instructions for installing these certificates into the keychain on their computer. Refer to Apple support documentation for instructions on how to manually install certificates into the keychain on the computer.

iOS

For devices running iOS, you can use a mobile device management solution to distribute and install trusted CA certificates on managed iOS devices. Refer to the support documentation for your mobile device management solution for detailed instructions on how to deploy certificates to managed iOS devices.

For unmanaged devices, unless you use a well-known certificate vendor that is already trusted by the device, your users will need to install CA certificates themselves. You will need to make the CA certificates available to users and give them instructions for installing these certificates into the keychain on their device. Refer to Apple support documentation for instructions on how to manually install certificates into the keychain on the device.

Android

For devices running Android, you can use a mobile device management solution to distribute and install trusted CA certificates on managed Android devices. Refer to the support documentation for your mobile device management solution for detailed instructions on how to deploy certificates to managed Android devices.

For unmanaged devices, unless you use a well-known certificate vendor that is already trusted by the device, your users will need to install CA certificates themselves. You will need to make the CA certificates available to users and give them instructions for installing these certificates into the **Trusted credentials** store on their device. Refer to the Android device vendor's support documentation for instructions on how to manually install certificates into the **Trusted credentials** store on the device.

> *As of Android 4.4, Android devices which have had additional CA certificates installed may display a warning notification indicating that a third party is capable of monitoring the user's network activity, including emails, apps, and secure websites. You may need to educate your users that this notification is due to the installed CA certificate that is needed to operate in your network.*
>
> *All versions of Android will require the user to set a device lock mechanism (PIN or pattern) when additional CA certificates are installed. Users should already have a device lock mechanism configured in order to protect any enterprise data on their device, however some users may not have followed this security best practice. You may need to educate users that using the device lock mechanism is a security requirement in order to protect enterprise data on their device.*

Avaya desk phones

Avaya desk phones such as the 9600 series IP deskphones have a mechanism for distributing the set of trusted CA certificates through the settings file downloaded from the utility server. You will need to make the CA certificates available on the utility server and include the appropriate configuration items in the settings file for the certificates to be downloaded to the phones. Refer to the `TRUSTCERTS` parameter in the *Administering Avaya IP Deskphones* document available at www.avaya.com/support for more details.

Certificate reference

In general, certificates should comply with RFC 5280 and current NIST recommendations, including:

- Using a recommended key algorithm;
- Using a recommended key length;
- Using a recommended message digest algorithm to create the certificate signature.

At time of writing, the current NIST recommendations were available at:
http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf

There are several classes of certificates used within the Avaya Unified Communications solution portfolio:

- Web services (server) – used by the Avaya Realm Mapper, Avaya Aura Conferencing web conferencing and document server, Personal Profile Management (a service on the Avaya Aura Session Manager), Avaya Multimedia Messaging, and the Utility Server, as well as various management interfaces.
- SIP server – from a client perspective, the primary concern is the Avaya Aura Session Manager; however from a solution perspective many network elements have SIP connections to the Avaya Aura Session Manager.
- XMPP server – primarily between clients and the Avaya Aura Presence Server for instant messaging, however there are other elements which use XMPP to connect with the Avaya Aura Presence Server.
- LDAP server – while your enterprise LDAP server is not technically part of the Avaya Unified Communications solution, a number of clients and network elements are able to connect to your enterprise LDAP server for directory information.
- "Generic" – this catch-all category encapsulates the Avaya one-X Client Enablement Services Handset Server as well as many internal management interfaces within the solution.

Each class of certificate has some specific details to consider that are captured in the sections below.

Most certificate vendors and the Avaya Aura System Manager interface provide a streamlined process for obtaining standard certificates. If you use this streamlined process, you must make sure of the following minimum requirements:

- The Subject Common Name field must include the fully-qualified DNS domain name of the server.
- The key algorithm and key size are compatible with your security policy
- The Subject Alternative Name field must have the following entries:
    - `ipAddress` – must have the IP address of the server
    - `dNSName` – must contain the fully-qualified DNS domain name of the server
    - `dNSName` – if the certificate is used for a SIP service, it must contain a `dNSName` entry containing the SIP domain being used. If multiple SIP domains are in use, you must have one `dNSName` entry for each SIP domain.
    - `uniformResourceIdentifier` – if the certificate is used for a SIP service, it must contain a `uniformResourceIdentifier` entry containing the SIP domain being used. If multiple SIP domains are in use, you must have one `uniformResourceIdentifier` entry for each SIP domain.

Wildcards are not supported for SIP domain entries.

Web service (server) certificates

Attribute	Value	Required?
Subject	`CN={fqdn}`	required
Validity	*validity period*	required
Authority Key Identifier	*hash*	required[1]
Subject Key Identifier	*hash*	recommended
Subject Public Key Info	*public key algorithm*	required
	public key data	required
Signature	*signature algorithm*	required
	signature value	required
Key Usage	`digitalSignature`	optional[2]
	`nonRepudiation`	optional[2]
	`keyEncipherment`	optional[2]
	`dataEncipherment`	optional[2]
Extended Key Usage	`id-kp-serverAuth = 1.3.6.1.5.5.7.3.3.1`	required
	`id-kp-clientAuth = 1.3.6.1.5.5.7.3.3.2`	optional[3]
Subject Alternative Name	`IP:{ip}`	optional[4]
	`DNS:{fqdn}`	required[5]
Authority Information Access	`OCSP - URI:http://{ocsp-server}{:ocsp-port}{/ocsp-path}`	optional
CRL Distribution Points	`URI:http://{crl-server}{:crl-port}{/crl-path}`	optional
	`URI:ldap://{crl-server}{:crl-port}{/crl-dn}`	optional

[1] authority key identifiers are required elements in end entity certificates to establish a trust chain.
[2] values may vary as specified in RFC 5280 and RFC 3279.
[3] required if the same identity certificate is used when the server is acting as a client.
[4] for the 96xx endpoints, PPM is "always" defined as an IP address, so PPM certificates must contain the `IP:{ip}` Subject Alternative Name entry when these endpoints are part of the solution.
[5] if the `CN` field of the Subject contains the fully-qualified domain name of the server, then the `DNS:{fqdn}` entry in the Subject Alternative Name is optional.

Web service certificate references

- RFC 2818 (2000), HTTP Over TLS

Special notes

- Wildcard name matching is defined in RFC 2818.

SIP server certificates

Attribute	Value	Required?
Subject	`CN={fqdn}`	required
Validity	*validity period*	required
Authority Key Identifier	*hash*	required[1]
Subject Key Identifier	*hash*	recommended
Subject Public Key Info	*public key algorithm*	required
	public key data	required
Signature	*signature algorithm*	required
	signature value	required
Key Usage	`digitalSignature`	optional[2]
	`nonRepudiation`	optional[2]
	`keyEncipherment`	optional[2]
	`dataEncipherment`	optional[2]
Extended Key Usage	`id-kp-serverAuth = 1.3.6.1.5.5.7.3.3.1`	required
	`id-kp-clientAuth = 1.3.6.1.5.5.7.3.3.2`	optional[3]
	`id-kp-sipDomain = 1.3.6.1.5.5.7.3.20`	contraindicated[4]
Subject Alternative Name	`IP:{ip}`	optional
	`URI:sip:{domain}`	required[5]
	`DNS:{domain}`	required[5]
	`DNS:{fqdn}`	required[6]
Authority Information Access	`OCSP - URI:http://{ocsp-server}{:ocsp-port}{/ocsp-path}`	optional
CRL Distribution Points	`URI:http://{crl-server}{:crl-port}{/crl-path}`	optional
	`URI:ldap://{crl-server}{:crl-port}{/crl-dn}`	optional

[1] authority key identifiers are required elements in end entity certificates to establish a trust chain.
[2] values may vary as specified in RFC 5280 and RFC 3279.
[3] required if the same identity certificate is used when the server is acting as a client.
[4] validation of the presence of the `id-kp-sipDomain` EKU as described in RFC 5924 is discouraged, as it limits use of the certificate to SIP only and forces certificate proliferation.
[5] the 96xx endpoints require the SIP domain to be present in the Subject `CN` or as a `DNS:{domain}` entry in the Subject Alternative Name field. Not checked for server-to-server.
[6] if the `CN` field of the Subject contains the fully-qualified domain name of the server, then the `DNS:{fqdn}` entry in the Subject Alternative Name is optional.

SIP certificate references

- RFC 5922 (2010), Domain Certificates in the Session Initiation Protocol (SIP)
- RFC 5924 (2010), Extended Key Usage (EKU) for Session Initiation Protocol (SIP)

Special notes

- Wildcards are explicitly disallowed in RFC 5922.

XMPP server certificates

Attribute	Value	Required?
Subject	`CN={fqdn}`	required
Validity	*validity period*	required
Authority Key Identifier	*hash*	required[1]
Subject Key Identifier	*hash*	recommended
Subject Public Key Info	*public key algorithm*	required
	public key data	required
Signature	*signature algorithm*	required
	signature value	required
Key Usage	`digitalSignature`	optional[2]
	`nonRepudiation`	optional[2]
	`keyEncipherment`	optional[2]
	`dataEncipherment`	optional[2]
Extended Key Usage	`id-kp-serverAuth = 1.3.6.1.5.5.7.3.3.1`	required
	`id-kp-clientAuth = 1.3.6.1.5.5.7.3.3.2`	optional[3]
Subject Alternative Name	`IP:{ip}`	optional
	`DNS:{fqdn}`	required[5]
	`SRV:_xmpp-client.{domain}`	optional[4]
	`SRV:_xmpp-server.{domain}`	optional[4]
Authority Information Access	`OCSP - URI:http://{ocsp-server}{:ocsp-port}{/ocsp-path}`	optional
CRL Distribution Points	`URI:http://{crl-server}{:crl-port}{/crl-path}`	optional
	`URI:ldap://{crl-server}{:crl-port}{/crl-dn}`	optional

[1] authority key identifiers are required elements in end entity certificates to establish a trust chain.
[2] values may vary as specified in RFC 5280 and RFC 3279.
[3] required if the same identity certificate is used when the server is acting as a client.
[4] RFC 6120 indicates that certificates should include SRV-ID identifiers as defined in RFC 4985 so that peers which are doing lookups using SRV records will be able to validate the certificates.
[5] if the `CN` field of the Subject contains the fully-qualified domain name of the server, then the `DNS:{fqdn}` entry in the Subject Alternative Name is optional.

XMPP certificate references

- RFC 6120 (2011), Extensible Messaging and Presence Protocol (XMPP): Core
- RFC 4985 (2007), Internet X.509 Public Key Infrastructure: Subject Alternative Name for Expression of Service Name

Special notes

- Wildcard matching is allowed by RFC 6120.

LDAP server certificates

Attribute	Value	Required?
Subject	`CN={fqdn}`	required
Validity	*validity period*	required
Authority Key Identifier	*hash*	required[1]
Subject Key Identifier	*hash*	recommended
Subject Public Key Info	*public key algorithm*	required
	public key data	required
Signature	*signature algorithm*	required
	signature value	required
Key Usage	`digitalSignature`	optional[2]
	`nonRepudiation`	optional[2]
	`keyEncipherment`	optional[2]
	`dataEncipherment`	optional[2]
Extended Key Usage	`id-kp-serverAuth = 1.3.6.1.5.5.7.3.3.1`	required
	`id-kp-clientAuth = 1.3.6.1.5.5.7.3.3.2`	optional[3]
Subject Alternative Name	`IP:{ip}`	optional
	`DNS:{fqdn}`	required[4]
Authority Information Access	`OCSP - URI:http://{ocsp-server}{:ocsp-port}{/ocsp-path}`	optional
CRL Distribution Points	`URI:http://{crl-server}{:crl-port}{/crl-path}`	optional
	`URI:ldap://{crl-server}{:crl-port}{/crl-dn}`	optional

[1] authority key identifiers are required elements in end entity certificates to establish a trust chain.
[2] values may vary as specified in RFC 5280 and RFC 3279.
[3] required if the same identity certificate is used when the server is acting as a client.
[4] if the `CN` field of the Subject contains the fully-qualified domain name of the server, then the `DNS:{fqdn}` entry in the Subject Alternative Name is optional.

LDAP certificate references

- RFC 4513 (2006), Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms

Special notes

- Wildcard name matching for LDAP DNS names is allowed by RFC 4513.

"Generic TLS" server certificates - anything else

Attribute	Value	Required?
Subject	`CN={fqdn}`	required
Validity	*validity period*	required
Authority Key Identifier	*hash*	required[1]
Subject Key Identifier	*hash*	recommended
Subject Public Key Info	*public key algorithm*	required
	public key data	required
Signature	*signature algorithm*	required
	signature value	required
Key Usage	`digitalSignature`	optional[2]
	`nonRepudiation`	optional[2]
	`keyEncipherment`	optional[2]
	`dataEncipherment`	optional[2]
Extended Key Usage	`id-kp-serverAuth = 1.3.6.1.5.5.7.3.3.1`	required
	`id-kp-clientAuth = 1.3.6.1.5.5.7.3.3.2`	optional[3]
Subject Alternative Name	`IP:{ip}`	optional
	`DNS:{fqdn}`	required[4]
Authority Information Access	`OCSP - URI:http://{ocsp-server}{:ocsp-port}{/ocsp-path}`	optional
CRL Distribution Points	`URI:http://{crl-server}{:crl-port}{/crl-path}`	optional
	`URI:ldap://{crl-server}{:crl-port}{/crl-dn}`	optional

[1] authority key identifiers are required elements in end entity certificates to establish a trust chain.
[2] values may vary as specified in RFC 5280 and RFC 3279.
[3] required if the same identity certificate is used when the server is acting as a client.
[4] if the `CN` field of the Subject contains the fully-qualified domain name of the server, then the `DNS:{fqdn}` entry in the Subject Alternative Name is optional.

Generic TLS certificate references

- RFC 5280 (2008), Internet X.509 Public Key Infrastructure Certificate & Certificate Revocation List (CRL) Profile

Sample server identity certificate

The example below shows a SIP server identity certificate with a 2048-bit RSA key signed using the SHA-256 signature algorithm for a server with DNS name `sip-server.example.com`, IP address `10.0.0.2`, and SIP domain `sip.example.com`.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            88:7e:4c:9c:5a:bd:e5:90
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Avaya, OU=Samples, CN=Sample root CA
        Validity
            Not Before: May 18 18:20:06 2014 GMT
            Not After : May 18 18:20:06 2015 GMT
        Subject: C=US, O=Avaya, CN=sip-server.example.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                  ...
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Key Usage:
                Digital Signature,
                Non Repudiation,
                Key Encipherment,
                Key Agreement
            X509v3 Extended Key Usage:
                TLS Web Server Authentication,
                TLS Web Client Authentication
            X509v3 Subject Key Identifier:
                AC:...
            X509v3 Authority Key Identifier:
                keyid:...
            X509v3 Subject Alternative Name:
                URI:sip:sip.example.com,
                DNS:sip.example.com,
                DNS:sip-server.example.com,
                IP Address:10.0.0.2
            Authority Information Access:
                OCSP - URI:http://ocsp.example.com

    Signature Algorithm: sha256WithRSAEncryption
      ...
```

Choosing a certificate vendor

There are many certificate vendors in the marketplace, and it can be difficult to know how to choose among them. This section will give you some questions to ask that should help you create some criteria to evaluate the various vendors and make a decision.

There are other basic considerations that you should take into account, such as certificate lifetime, service level agreements for revocation checking, and support terms among others, but the following are some questions that we have found useful as additional detail when comparing vendors.

Q1 – Is your root certificate included in the default platform trust store for the operating systems we use?

Make sure that the vendor can issue certificates that will be trusted by the operating systems and devices that you are using. For example, you may need certificates that are trusted by iOS, Android, Microsoft Windows, and Mac OS X. It is a good idea to ensure that your vendor's certificates are trusted by the particular versions of the operating systems that your client devices are running.

Q2 – What is the base cost for each certificate?

The per-certificate base cost will be an important factor to consider when choosing a vendor. Certificate vendors have a wide range of cost structures, so it is a good idea to shop around.

Q3 – Do you support creating certificates with multiple Subject Alternative Name entries? What is the additional cost per alternative name?

Most certificates will require at least one and possibly multiple alternative names. Some vendors charge the same price for an alternative name entry as for an entire certificate, even if the alternative name doesn't reflect a separate server (for example, the SIP domain alternative name in SIP certificates).

Q4 – Do you support all of the Subject Alternative Name entry types that we need?

The standards for some protocols specify having particular entries in certificate Subject Alternative Name fields, like the SRV entries in XMPP certificates. These entries may be required for your servers to interoperate with solutions from other vendors. If you need these entries, it is important for your certificate vendor to be able to generate certificates that match your specifications.

Troubleshooting certificate problems

"The security certificate required for <...> is not installed"

If the user reports this message, it means that the server certificate is not trusted by their client device. To resolve this issue, ensure that the issuing CA certificate is installed on their device and that all certificates in the trust chain are valid.

"The security certificate required for <...> has expired"

If the user reports this message, it means that the server certificate or another certificate in the trust chain has expired. To resolve this issue, ensure that the server certificate and all certificates in the trust chain are valid.

"There is a <...> security certificate problem"

If the user reports this message, it means that the server certificate or another certificate in the trust chain has been revoked, is corrupted, or is not valid for the server. To resolve this issue, ensure that the server certificate and all certificates in the trust chain are valid and have the appropriate information required for proper validation.

References

Avaya product documentation

Avaya product documentation is available at https://support.avaya.com. To find the latest documentation for a particular product, visit the website and search for the name and release of the product.

Avaya provides a telephone number for you to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: www.avaya.com/support.

External standards

- RFC 2560 (2013), X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP)
- RFC 5246 (2008), Transport Layer Security (TLS) Protocol - Version 1.2
- RFC 5280 (2008), Internet X.509 Public Key Infrastructure Certificate & Certificate Revocation List (CRL) Profile
- *ITU-T Recommendation X.509 (2012), Information Technology - Open Systems Inter-connection - The Directory: Public-Key and Attribute Certificate Frameworks*