An Introduction To Intel® AMT Remote Configuration Certificate Selection

Guidelines for choosing the correct remote configuration (RCFG) certificate for your remote provisioning needs

White Paper

Version 2.01

Intel® vPro Technology™ Featuring Intel® AMT

Remote Configuration Certificates

Overview

Intel® Active Management Technology (Intel® AMT), a feature of Intel® vPro™ technology, offers a wide range of built-in platform capabilities and plug-ins for management and security applications to allow IT to better discover, heal, and protect their network computing assets. In order to take advantage of these capabilities, a client Intel® AMT computer must first be set up and configured to work in the enterprise network. This is commonly referred to as "being provisioned."

There are different methods that can be used to provision a client system. Most provisioning methods require physical interaction with the client system. However, remote configuration is a provisioning option that allows a client system to be provisioned with zero physical interaction. Remote configuration is ideal for systems that have already been deployed into an environment—but have not yet been provisioned—allowing IT to provision systems without visiting each system individually.

To use remote configuration for provisioning a system, a special remote configuration (RCFG) certificate is needed. Section I of this white paper gives a high level explanation about the remote configuration certificate. Section II of the paper goes into more detail on what is required in using the RCFG certificate. Section III explains the different types of RCFG certificates, shows examples of how the different certificate types would work in an environment, and helps determine which RCFG certificate type works in your network environment.

Table of Contents

Introduction

Remote Configuration is used during the provisioning process between an Intel® AMT client computer and a provisioning server. Below is a high level overview of the process steps that automatically take place when remote configuration is used. Details pertaining to these steps are described in this document.

1. Provisioning server receives "Hello" message from Intel® AMT client computer. This initiates the provisioning process.
2. Client computer asks provisioning server for RCFG certificate.
3. Provisioning server sends client RCFG certificate with the certificate's full chain of trust including the root certificate. This root certificate would reflect the certificate authority vendor used and will include the certificate authority vendor's thumbprint.
4. Client computer parses the RCFG certificate, verifies that the chain of trust is not broken, extracts the root certificate thumbprint and compares it against the thumbprint's table present in the client's Intel® AMT FW. Provisioning stops here if no match is found.
5. Client computer gets domain from DHCP Option 15 setting and verifies this suffix matches the CN field from the certificate. The way a match is determined depends on the client computer's Intel® AMT firmware version and the RCFG certificate type used. Provisioning stops here if no match is found.
6. Remote Configuration certificate is now successfully verified and provisioning process continues as normal.

This document covers remote configuration for the following Intel® AMT firmware versions: 2.2, 2.6, 3.x, 4.x, 5.x, 6.x and 7.x. Future revisions of Intel® AMT firmware may support additional functionality that is not covered in this document.

Acronym	Expanded Form
CA	Certificate Authority
CN	Common Name
CSR	Certificate Signing Request
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
FQDN	Fully Qualified Domain Name
FW	Firmware
Intel® AMT	Intel® Active Management Technology
Intel® ME	Intel® Management Engine (Intel® vPro™ Technology BIOS Extension)
OID	Object Identifier
OU	Organizational Unit
RCFG	Remote Configuration
SSL	Secure Socket Layer
TLD	Top Level Domain
TLS	Transport Layer Security
UCC	Unified Communication Certificate

Figure 1. Acronyms used in this document

Section I: Digital Security Certificates

This section describes digital security certificates and then outlines the particular certificate required for remote configuration of Intel® AMT.

What is a Certificate?

A certificate is an electronic document which contains identification information and can be used to establish secure and authenticated communication between computers.

A good analogy for understanding these certificates is to compare them with passports. In the same way a passport can be used to identify a person, a certificate on a computer can be used to identify a computer or a website.

For example, imagine a person going on a trip who needs to go through customs. Before going on the trip, the individual must get a passport issued from the passport agency. The passport agency verifies the person's identity and issues a passport specific for that person. When the person is actually going through customs, the customs officer knows nothing about the person; however, the customs officer does trust the passport agency. When the individual supplies a passport issued from the passport agency to the customs officer, the customs officer trusts that passport correctly identifies the person. This helps create a "chain-of-trust". Even though the customs official has no trust established with the individual, they do trust the passport agency and the passport itself.

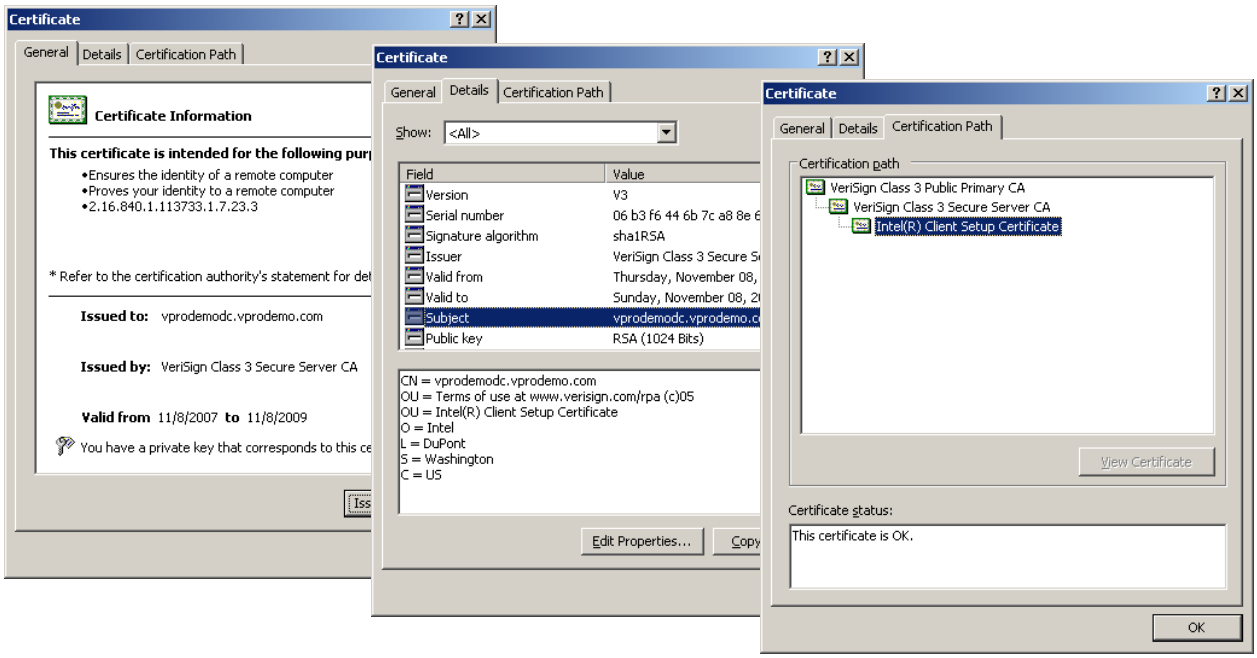

Figure 2. An example of what a certificate looks like on your computer system.

A certificate for your computer operates on a similar principle. When a company is planning on creating a secure website, the company needs to get a certificate issued from a certificate authority. The certificate authority verifies the company's identity and issues a certificate specific for that company. When an end-user goes to the company's website, the end-user might know nothing about the company, however, the end-user does trust the certificate authority. When the company's website supplies a certificate issued from the certificate authority to the end-user, the end-user trusts the certificate correctly identifies the company's website.

To see an example of a certificate in use, go to a "secure" website, like the websites used to log into banking information or used to complete a credit card transaction on the internet. Secure websites usually will display a lock icon in the browser screen. If you double click this icon you can see the certificate for the website.

A certificate is created based on a set of input parameters that may include: the intended functionality of the certificate, the name of the certificate, and the name of the company. Certificates are issued by certificate authorities like Comodo*, Go Daddy*, Starfield*, or VeriSign*. Certificate authorities are trusted third party organizations that issue certificates. One of the functions certificate authority vendors provide is verifying the accuracy of identifying information, such as a company's name. If inaccurate or incomplete information is submitted, the certificate authority vendor will not issue a certificate.

The Remote Configuration Certificate

A remote configuration certificate is used specifically to establish secure and authenticated communication between a provisioning server and an Intel® AMT client computer to be provisioned. There are currently four main types of certificates that are supported for remote configuration:

- Standard SSL Certificate
- Wildcard (*) Certificate
- Unified Communication Certificate (UCC)
- Multi-level domain only support

The best certificate to use depends on the overall environment where the remote configuration provisioning solution is being deployed. Different certificates are supported in different environments, and each certificate has a different pricing model.

Each certificate type will be discussed in detail in Section III.

Keep in mind that the remote configuration certificate is only used for the initial provisioning of an Intel® AMT client that is provisioned using remote configuration. The remote configuration certificate is separate from the certificates needed for secure communications such as the certificates for TLS, Mutual TLS, 802.1x, or the SSL certificate for web services. These web services certificates are options for advanced Intel® AMT provisioned system management. For more information on these read about Advanced provisioning in Intel® AMT / Intel® Management Engine (Intel® ME) configuration at http://communities.intel.com/docs/DOC-1684.

Every certificate has a chain of trust to a root certificate. The root certificate identifies where the certificate was issued from. Part of this root certificate is a "thumbprint", also called a hash value, which is a unique identifier that corresponds to the identity of the certificate issuer. When you purchase a certificate from a certificate authority vendor—like VeriSign, the certificate receives a thumbprint from that certificate authority vendor. Intel® AMT firmware on client systems contains a table that lists thumbprints that are supported for remote configuration. By purchasing a certificate from one of the pre-approved certificate authority vendors, the certificate will match the table built into the Intel® AMT firmware and remote configuration can happen.

The certificate authority vendors offer many different certificate packages and options. Some features such as an Extended Validation (EV) certificate may not be required for your remote configuration needs. Be sure to discuss your remote configuration requirements with your certificate authority vendor so that you can determine the best certificate for your environment.

More advanced options allow additional thumbprints to be added to Intel® AMT clients, but are out of scope for this paper.

Section II: Certificate Setup

This section provides more detail on the remote configuration certificate and the processes required to use it to remotely configure Intel® AMT clients. Areas covered include certificate parameters, commercially available certificates, Intel® AMT firmware revisions, details on the importance of DHCP option 15, and a discussion on how domain layout affects remote configuration.

Certificate Parameters

Certificate requests are generated from a specific set of input parameters. In this section we will discuss fields required in the input parameters.

There are some common fields that need to be set in the certificate to identify it as a remote configuration certificate. There are two options (shown in Figure 3 & 4) that can be used to identify a certificate as a remote configuration certificate:

Option 1) Set the OID in the **enhanced** key usage field with:
1.3.6.1.5.5.7.3.1 (standard OID for Server Authentication Certificate)
2.16.840.1.113741.1.2.3 (custom OID for Intel setup extension)

Option 2) Set the OID in the **extended** key usage field with:
1.3.6.1.5.5.7.3.1 (standard OID for Server Authentication Certificate)
Set the OU value in the Subject field with "Intel® Client Setup Certificate"

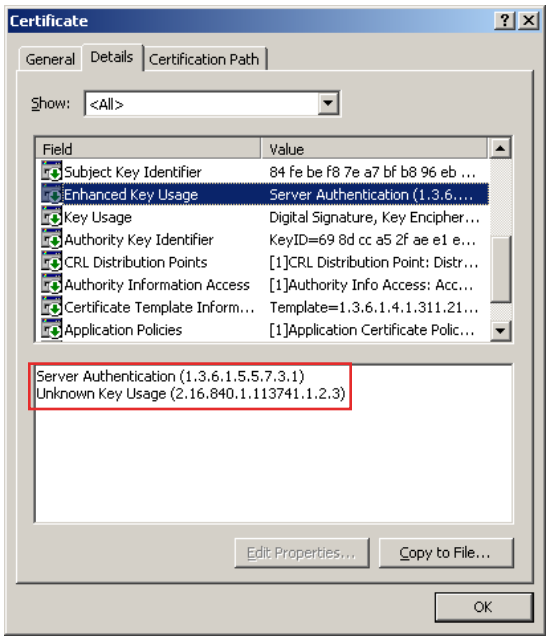

Figure 3. RCFG Certificate Parameters Option 1

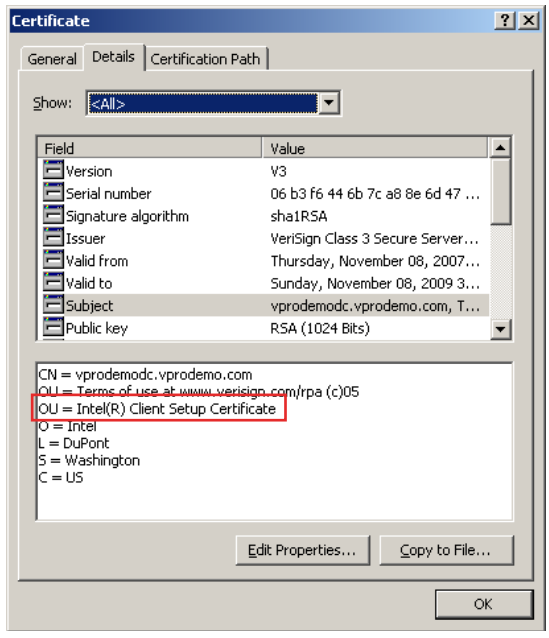

Figure 4. RCFG Certificate Parameters Option 2

Platform	Supported Firmware Versions	RCFG Certificate Support
2006 Desktop system (based on Intel® Q965 Express Chipset)	2.2	Standard SSL Only
2007 Mobile system (based on Mobile Intel® GM/PM965 Express Chipset)	2.6	Standard SSL (with Multi Level Domain*), Wildcard, and UCC
2007 Desktop system (based on Intel® Q35 Express Chipset)	3.2	Standard SSL (with Multi Level Domain*), Wildcard, and UCC
2008 Mobile system (based on Mobile Intel® GM/PM45 Express Chipset)	4.x	Standard SSL (with Multi Level Domain*), Wildcard, and UCC
2008 Desktop system (based on Intel® Q45 Express Chipset)	5.x	Standard SSL (with Multi Level Domain*), Wildcard, and UCC
2010 Desktop system (based on Intel® Q57 Express Chipset)	6.x	Standard SSL (with Multi Level Domain), Wildcard, and UCC
2011 Desktop system (based on Intel® Q67 Express Chipset)	7.x	Standard SSL (with Multi Level Domain), Wildcard, and UCC

*Intel® AMT versions 2.6, 3.2, 4.0, and 5.0 only support up to second level .net and .com domains. Refer to section III for more details.
Figure 6. Intel® AMT Firmware Generations

Which option to use to identify a remote configuration certificate depends on the certificate vendor from whom you are purchasing the configuration certificate. Some vendors do not support custom OIDs, while other vendors prefer the custom OID value over the OU setting. Figure 5 lists the certificate vendors supported at the time this document was published.

In addition to identifying the certificate as a remote configuration certificate using one of the above options, the certificate must be set for the domain in which it will be used. This is accomplished by setting the Subject field CN parameter with the fully qualified domain name of the domain using remote configuration. In the Certificate Types section later in this document, we talk more about what the CN parameter should be set to based on the overall domain structure and the certificate type being used.

Requesting a Certificate From a Certificate Authority Vendor

Intel® AMT Firmware (FW) supports the following certificate authority vendors by default (other vendor thumbprints can be added manually):

Certificate Vendor	Website
Comodo*	http://www.comodo.com/intel/
Go Daddy*	http://help.godaddy.com/topic/235/article/5260
Starfield*	http://www.starfieldtech.com/
Verisign*	http://www.verisign.com/ssl/intel-vpro-technology/index.html
Entrust*+	http://www.entrust.com/
Cybertrust*+	http://www.verizonbusiness.com

Figure 5. RCFG Certificate Vendors

+ Support for Cybertrust certificates starts with Intel® AMT version 6.1. Entrust certificates support starts with Intel® AMT version 7.x. To confirm certificate support run the Intel® AMT Diagnostics tool at http://communities.intel.com/docs/DOC-5582.

Each certificate authority vendor can accept a Certificate Signing Request or CSR for requesting a new certificate. A CSR is a standard file all the above certificate vendors accept. The CSR contains all of the parameters for a certificate including the CN, OU, and OID fields specified above, in addition to identifying information for the specific organization requesting the certificate.

Each certificate authority vendor provides different levels of support and cost models. Your individual business needs will determine which vendor to use. It is highly recommended to work with the customer service of the certificate authority vendors to determine which vendor is correct for you.

Intel® AMT Firmware Versions

The Intel® AMT firmware version of a client system is dependent upon the hardware of the individual system itself. An enterprise environment can be comprised of a mix of platforms—all with different Intel® AMT firmware versions.

The Intel® AMT firmware versions of the systems to be provisioned plays an important part in determining which type of certificates can be used for Remote Configuration.

Above is a table (Figure 6) that summarizes the firmware versions by platform type and what certificates support them.

The firmware version on a system can be upgraded, but only to a firmware version supported by that platform. For example, if you have a 2006 Desktop system you can upgrade the firmware from version 2.1 to version 2.2. You could not upgrade the firmware to version 3.0.

The **Intel® AMT Diagnostics tool** is a utility that can be used to locate the Intel® AMT version of your system and can be used to locate the certificate authority vendors that your client system supports. The utility can be downloaded at http://communities.intel.com/docs/DOC-5582.

DHCP Option 15

Remote configuration uses DHCP Option 15 "DNS domain name option" to determine the domain a client computer belongs to. The DHCP server(s) must be correctly configured to support this option. Using DHCP, the Intel® AMT client system will discover its own domain and verify its domain matches the CN field listed in the remote configuration certificate.

How Do I Determine Intel® AMT FW Version and DHCP Option 15?

The **Intel® Remote Configuration Certificate Scout** is a simple command line utility that allows users to query a system to detect Intel® AMT Firmware version and DHCP option 15 "DNS domain option name" settings. This utility supports Intel® AMT systems, and will work on either provisioned or unprovisioned systems. This will give you information about the single system under test.

Requirements

Supports the following Microsoft* operating systems:

- Windows* XP
- Windows* Vista (any version)
- Windows* 7 (any version)

The following device drivers must be installed and enabled:

- Intel® Management Engine Interface driver

For more information, please see Intel® Remote Configuration Certificate Scout.

Domain Structure

The domain structure for the systems to be provisioned depends entirely on how the IT infrastructure is set up. This domain structure will dictate what certificate types will be best supported.

The CN parameter in the remote Configuration Certificate must match the DHCP option 15 setting.

Below is an example (Figure 7) of how a domain could be set up. With this example we will show what certificates would be supported. The CN used in a certificate is based off of a registered TLD (.com, .net, .uk). When requesting a certificate the certificate authority vendor will verify that the owner of the requesting certificate matches the owner of the domain name (e.g. company.com). If the names do not match the issuing certificate authority vendor will contact the domain owner so that permission can be obtained.

In the following section the DHCP option 15 settings match the way the domain is set up. For example a DHCP server for Mkgt.East.Company.local would have the DHCP option 15 value set to Mkgt.East.Company.local. During remote configuration the DHCP option 15 value is used for authentication regardless of the domain the computer is logged in to.

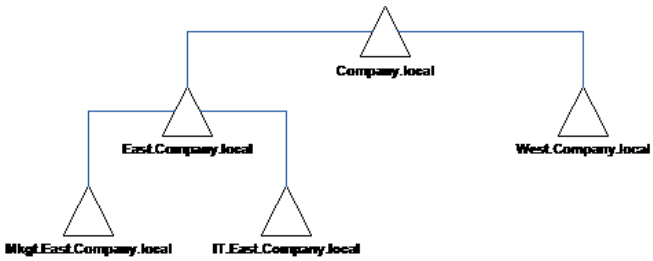

Figure 7. Example Domain

Section III: Certificate Types & Selection

This final section describes the different types of remote configuration certificates and presents a decision tree to help in determining which certificate(s) work best for your network environment.

Standard SSL Certificate

The Standard SSL Certificate is a basic type of certificate. The benefit of using standard certificates is that they are supported by all Intel® AMT FW versions that support remote configuration. The drawback of this certificate is that the certificate CN field must match the full domain suffix. This means that separate certificates will be required for each domain.

Using the example domain, if a Standard SSL certificate was purchased with the CN field set to <Server>.Mkgt.East.Company.local then only systems directly in that domain would be able to be remotely configured with this certificate (Figure 8). Systems in IT.East.Company.local would not be able to be remotely configured with this certificate because the full domain names do not match. Similarly, systems in West.Company.local would not be remotely configurable with this certificate. In order to remotely provision systems in IT.East.Company.local or West.Company.local additional certificates would need to be purchased for those domains.

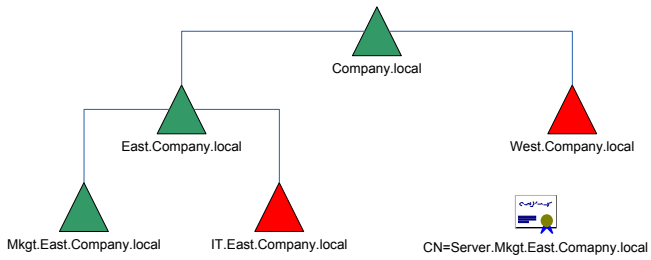

Figure 8. Standard SSL w/CN = <Server>.Mkgt.East.Company.local

If the CN field was set to <Server>.East.Company.local neither Mkgt.East.Company.local nor IT.East.Company.local would be supported (Figure 9).

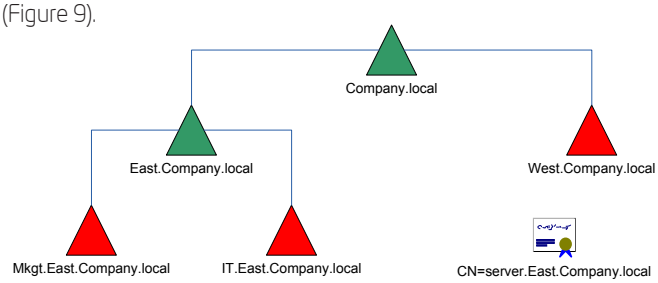

Figure 9. Standard SSL w/CN = <Server>.East.Company.local

If the CN field was set to <Server>.Company.local then none of the sub-domains would be supported (Figure 10).

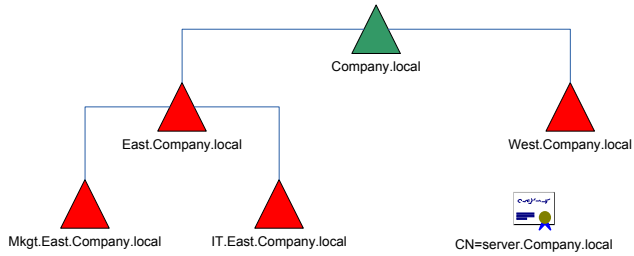

Figure 10. Standard SSL w/CN = <Server>.Company.local

Wildcard(*) SSL Certificate

Wildcard (*) SSL Certificates let you specify a domain set using a * character as a wildcard field. The benefit of using wildcard certificates is that only overlapping fields between the certificate CN field and the domain suffix need to match. This means one certificate is applicable across multiple parts of a domain forest. Wildcard certificates are not supported in Intel® AMT FW versions 2.5 and 3.0. Wildcard certificates can cost more than a single standard certificate, but may be more cost effective and easier to manage than multiple standard certificates.

Using the example domain (Figure 11), if a wildcard certificate was purchased with the CN field set to *.East.Company.local then all domains under and including East.Company.local would match. Company.local would match because all overlapping fields (in this case just "Company" and "local") match. West.Company.local would not match because the first overlapping field (west) does not match the CN.

If you purchased a wildcard certificate for *.Company.local then all nodes in this domain example would be covered.

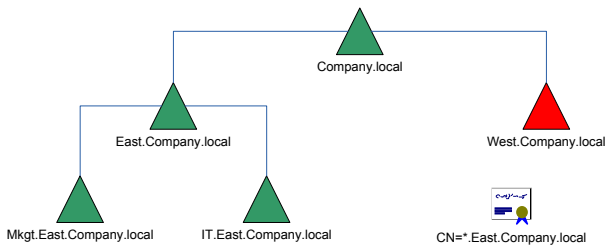

Figure 11. Wildcard (*) SSL w/CN = *.East.Company.local

Unified Communication Certificate (UCC)

A UCC also allows a single certificate to be applicable to multiple domains within a domain forest. Basically, a UCC allows you to specify a list of domains to be covered by the same certificate. UCC is not supported in Intel® AMT FW versions 2.2 and 3.0.

UCC's are purchased for a set list of domains, and can cover a wide range of domains for companies that have different root domains. A UCC's cost depends on the number of domains listed—the more domains the greater the cost. Also note that the purchase of a certificate is a one-time purchase. For example, you could list all your domains in the initial UCC purchase but you couldn't add another domain to that list later.

A UCC's cost effectiveness can vary. A UCC for 10 domains may be more cost effective then 10 Standard SSL certificates but may be less cost effective then a single wildcard certificate. A UCC for 5 domains may be more cost effective then a single wildcard certificate. However, a wildcard certificate would be more scalable for future subdomains than a UCC.

Using the example domain, if a UCC was purchased you could list exactly what domains you wanted supported. By putting Company.local, East.Company.local, West.Company.local, and Mkgt.East.Company.local on your UCC all of these domains would be covered. Any domain not listed in the UCC would not be supported (Figure 12).

If your company had a second domain like Company2.org you could also put that domain on the UCC list and cover multiple domain forests.

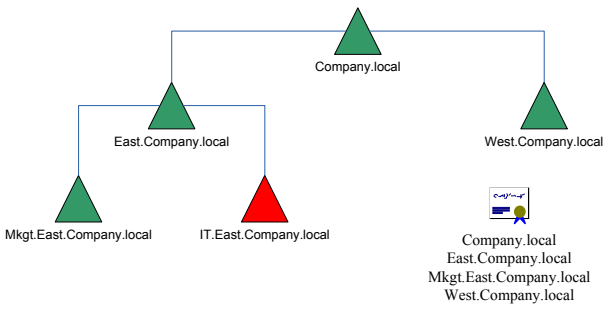

Figure 12. Unified Communication Certificate

Multi Level Domain And Country Code Support

Starting with Intel® AMT versions 2.6/3.2, .com and .net support was added as an extension of Standard SSL certificates. Country code TLD support and four additional geo TLDs support (.gov, .edu, .org, .arpa) were added to Intel® AMT 4.1/5.1 and later versions. This extended support typically requires only the TLD and second level (e.g. company.com) and if applicable the third level domain (e.g. company.co.uk) to match the CN field in the certificate. Country code domains, such as Japan, Australia, and Italy, that add additional complexity to their domain structures are not supported.

Looking back to the first example (Figure 8) using Standard SSL certificates where the certificate CN field is set to <Server>.Mkgt.East.Company.local, only the systems directly in that domain were supported and systems in IT.East.Company.local and West.Company.local were not supported.

In contrast to the Standard SSL certificates used in the earlier example, when configuring systems with Intel® AMT firmware that support multi-level domains, a standard certificate with CN field set to <Server>.Mkgt.East.Company.com would support all nodes in our domain example (Figure 13). Because the TLD ".com" and second level "Company" match for all of the domains, all of the domains shown would be supported. For a list of supported TLDs and additional examples refer to the "Intel® vPro™ Remote Configuration Domain Suffix Guide" at http://communities.intel.com/docs/DOC-4903

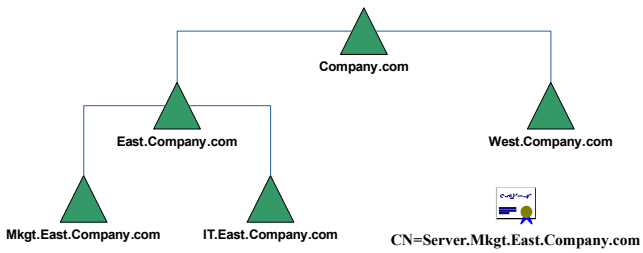

Figure 13. Second Level Domain Only Support

Picking the Right Certificate

The flowchart on the following page is a guideline that can help you determine which certificate type is recommended based on your environment. Due to variations in the number of domains being purchased and certificate vendor pricing models, we advise you to compare all options before buying any certificate.

Using the Certificate

Once you have selected and obtained your certificate(s) for remote configuration you can apply the certificate to your remote configuration solution. Some examples of solutions capable of taking advantage of Intel® AMT remote configuration include LANDesk* Management Suite, Altiris* Client Manager Suite, Microsoft* Systems Management Server (SMS) using Intel® AMT Setup and Configuration Service (Intel® SCS), Microsoft System Center Configuration (SCCM), and Intel® SCS Console.

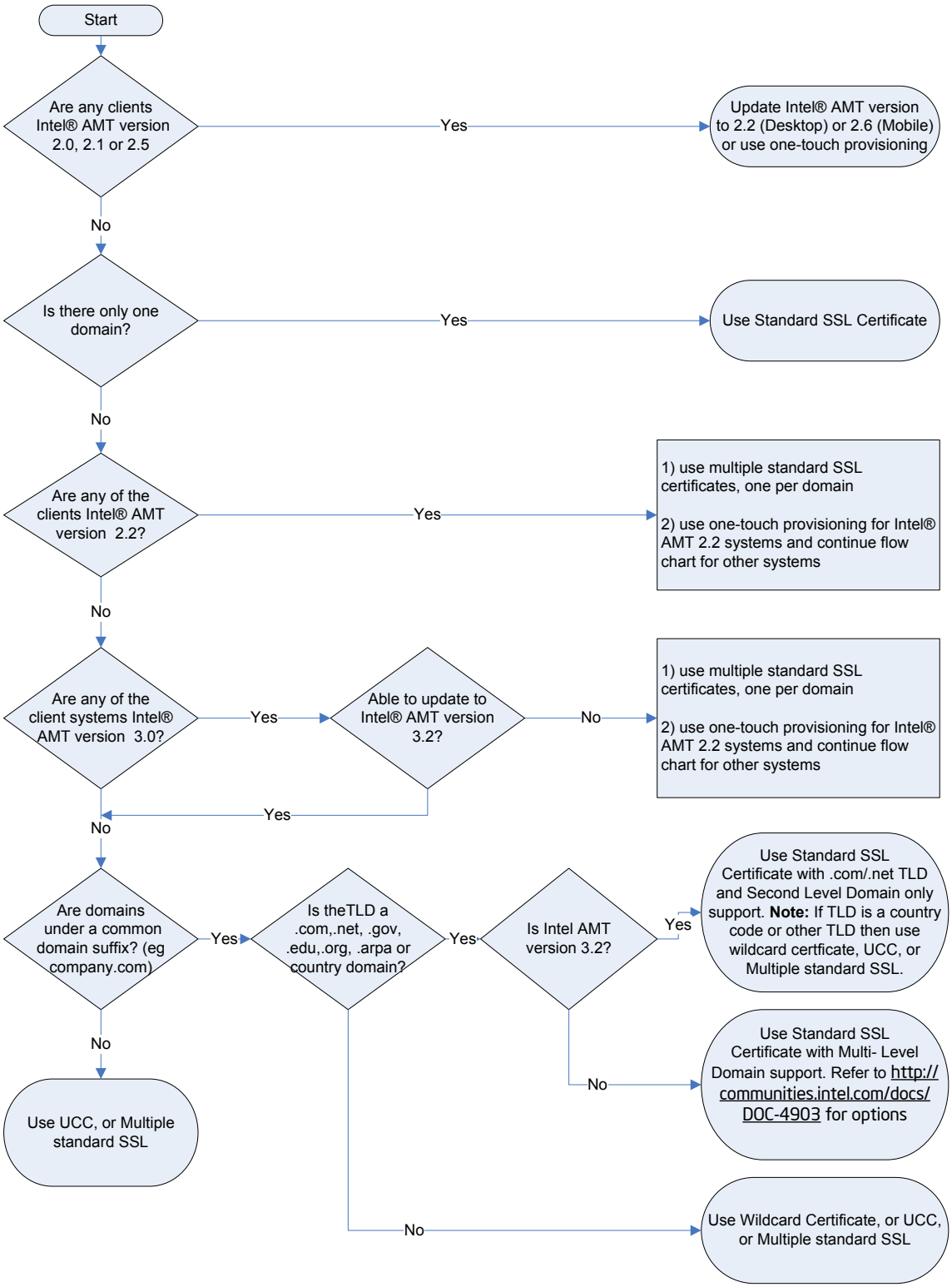

Figure 14. Certificate Selection Flowchart

References

The Intel® vPro™ Remote Configuration Domain Suffix Guide discusses in depth how Intel® AMT compares the certificate CN to the provisioning server's FQDN for remote configuration. Contains a list of supported TLDs: http://communities.intel.com/docs/DOC-4903

A compilation of links for all Intel® vPro™ technology certificates:
http://communities.intel.com/docs/DOC-2225

To learn more about Intel® AMT and Intel® vPro™ technology visit the following sites:

Utilities for Intel® vPro™ Technology

Intel® vPro™ Expert Center

Manageability Software Development Forum