Access Control Beyond MAC Address Filtering

How Digital Certificates help

Soliton®

Table of Contents

1. What is MAC address filtering (and why is it ineffective)?

This chapter will explore the basics of MAC address filtering, why it's commonly used, and its limitations as a security measure.

What is a MAC address?

MAC address stands for Media Access Control Address, and it's a unique identifier that devices need to communicate with a network segment such as Wi-Fi, Bluetooth and Ethernet.

MAC addresses typically consist of six groups of hexadecimal digits separated by hyphens or colons:

MM:MM:MM:SS:SS:SS

MM-MM-MM-SS-SS-SS

MMM.MMM.SSS.SSS

As every device has its unique MAC address, the number is often used to identify users and determine user rights. If a MAC address is whitelisted, the device is allowed to gain access to (a segment of) the network, and if it's not, access remains blocked. This process is called MAC address filtering.

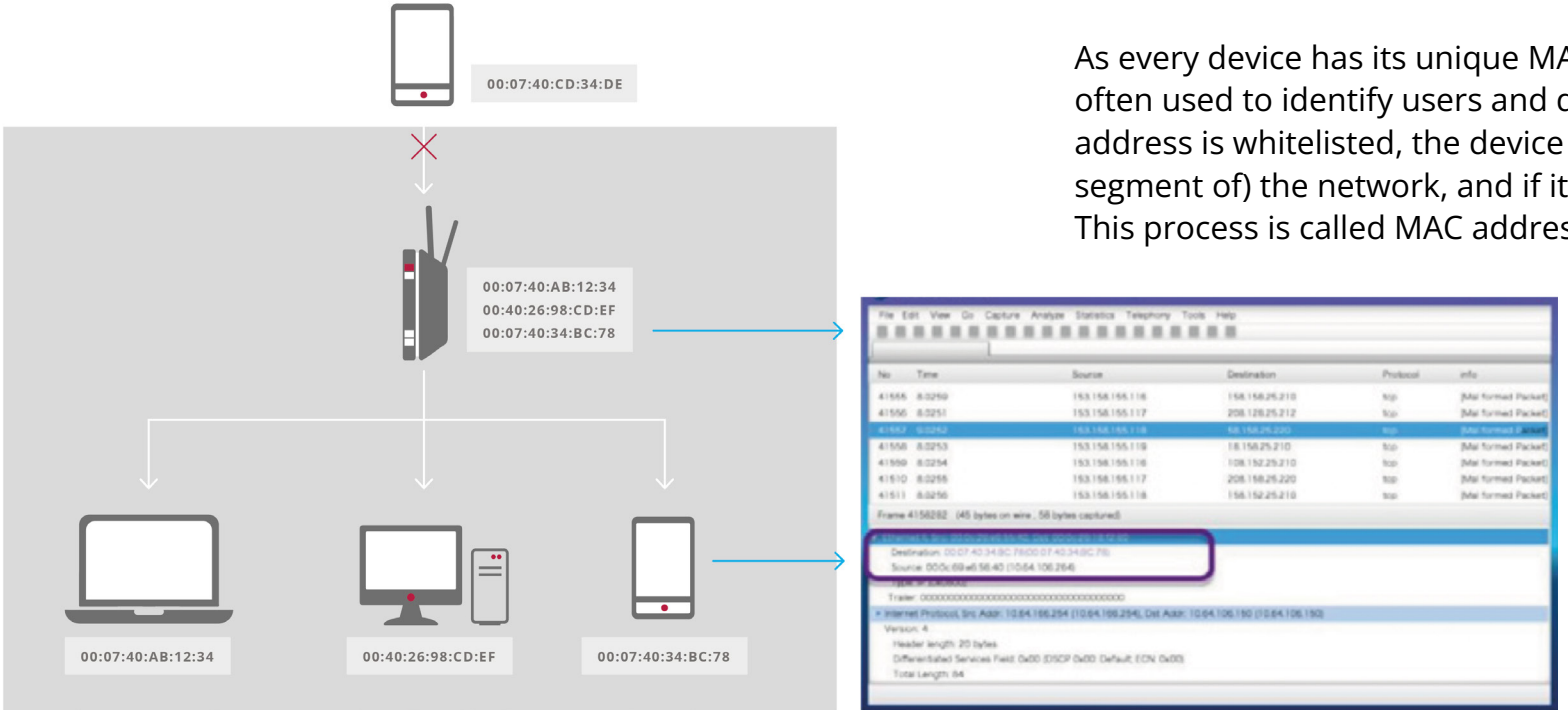


FIGURE: MAC ADDRESSES ARE NOT ENCRYPTED ON THE NETWORK

The problem with MAC address filtering

MAC address filtering is also called MAC address authentication as if it were an authentication method. Many people, therefore, believe that MAC address filtering is a reliable security measure. But it's not; MAC address filtering has a limited impact on protecting companies from cyberattacks. In fact, it's not officially a security matter at all. Instead, MAC address filtering gives people a false sense of security, which tells attackers that the network security is not strictly managed.

One of the main reasons MAC address filtering is dangerous is the risk of impersonation. MAC addresses are not encrypted on the network, so outsiders can identify them by capturing packets from the LAN.

Tools to change MAC addresses are distributed on the Internet and readily available. Hence, malicious attackers can effortlessly get past the security system by using these tools to "spoof" (falsify) the MAC address. Yes, attackers must decrypt encrypted communication or perform other tasks after getting past the security system. However, most common security measures are easily circumvented when hackers spoof a MAC address.

Long story short:

MAC address filtering is not a solid IT security measure and should only be used as a fallback mechanism if other methods cannot be applied. Now that targeted cyberattacks are becoming increasingly sophisticated, it's time for IT managers to take back control, find proactive security measures and move beyond MAC address filtering.

Before discussing these measures, let's first rule out some other security measures that all companies should cross off their list.

Obsolete security measures

Besides MAC address filtering, organisations sometimes still use outdated security measures, such as WEP encryption, stealth SSID (SSID broadcast OFF, rejection of “any connection”), and WPA2-PSK. These were all standard security measures for wireless LAN in the past. Today, however, they can no longer ensure sufficient security. WEP was never very effective in securing wireless data, and anyone can acquire SSID information from wireless clients even if stealth SSIDs are used.

The challenges with WPA2-PSK

Even WPA2-PSK, which is generally believed to be more robust, has a security hole. The PSK (pre-shared key) can be easily redisplayed and checked on the device where it’s set. Once attackers acquire the PSK, they can decrypt information in real-time by capturing wireless communication.

The operational issue

WPA2-PSK also has an operational problem: it doesn’t support so-called blacklist registration. Losing the PSK is like losing your house key: if it happens, you need to change the PSK on all the devices where it’s registered.

Operational load

This scenario causes a huge operational load, especially when your company has over 100 employees. Security measures for corporate wireless LAN are outdated and insufficient, both systematically and technologically. At the same time, the era of unmanaged devices and remote working means IT security is even more complex.

2. If all of this doesn't work - then what does?

In this chapter, we'll introduce IEEE 802.1X authentication, a more secure and robust alternative to MAC address filtering. You'll learn how it works, its benefits, and how it can be implemented to enhance the security of your network.

Now that we've crossed MAC address filtering, WEP encryption, stealth SSID, and WPA2-PSK off the list of solid security measures, what should you replace them with?

The answer lies in security measures based on IEEE 802.1X authentication, which blocks all communications from unauthenticated clients and only allows authenticated users to establish a connection. Components include the 802.1X-enabled LAN switch, a RADIUS authentication server, and an EAP authentication protocol.

EAP authentication

EAP-PEAP authentication uses an ID and password, and EAP-TLS uses electronic certificates. Specific authentication methods and their characteristics are shown in the table below. Here, EAP-TLS is desirable for corporate wireless LAN as it supports user and device authentication and can control connections from unauthorised devices. Because PEAP authentication cannot control personal smartphones, certificates are gaining popularity.

TLS authentication is being adopted in more and more cases. The encryption method used is WPA, and although it doesn't fix all security problems, the usage of IEEE 802.1X authentication does, making it a valuable combination.

To date, IEEE 802.1X authentication hasn't gained widespread acceptance. However, as the use of wireless LAN has spread among companies as the standard for network connections, more and more institutions report on the importance of IEEE802.1X authentication.

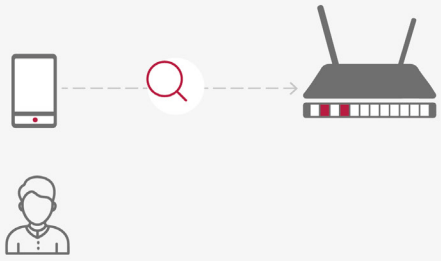
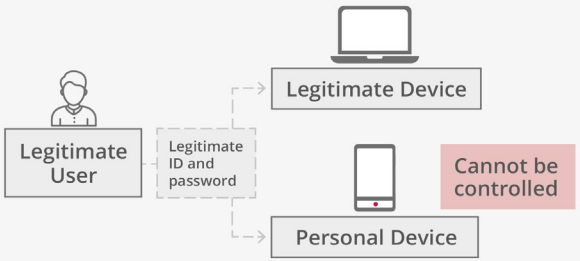
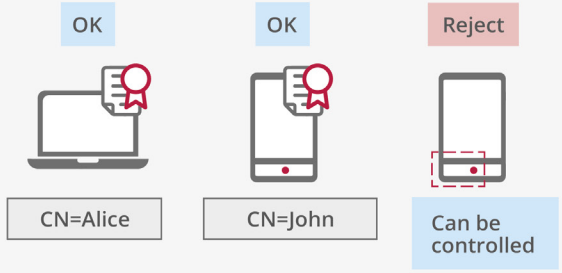
Authenication method	Shared WPA encryption key + MAC address filter	ID and password (EAP-PEAP authentication)	Digital certificate (EAP-TLS authenication)
Authenication strength	**Extremely Weak**	**Weak to Medium**	**Strong**
Advantages and disadvantages	The MAC Address can be stolen from the packet and esily spoofed. (Unauthorised access will not be noticed.) The MAC adress must be collected and deleted. 	If you know the password you can connect to the network from your personal device. Set-up that the user must perform is easy. 	User and device authentication (Control of connection from unauthorised devices) is supported. Digital certificates must be distributed. 
Suitable environment	**Home wireless router single base and small office.**	**Conventional IT environment where smartphones are not taken into consideration.**	**LAN in company or public office** LAN that contains personal data such as medical network.

FIGURE: COMPARISON WIRELESS LAN AUTHENTICATION

3. Getting Started with IEEE802.1X Authentication

In this chapter, we'll guide you through the initial steps of implementing IEEE 802.1X authentication on your network. You'll learn about the components needed for a successful implementation, the setup process, and best practices to ensure a smooth transition.

Now that you know about IEEE 802.1X authentication, let's look at its building process and the required functions.

IEEE 802.1X authentication is a so-called client authentication method, which means it's a method that blocks all communication from unauthenticated clients and only allows authenticated users and devices to establish contact.

Here's how it works:

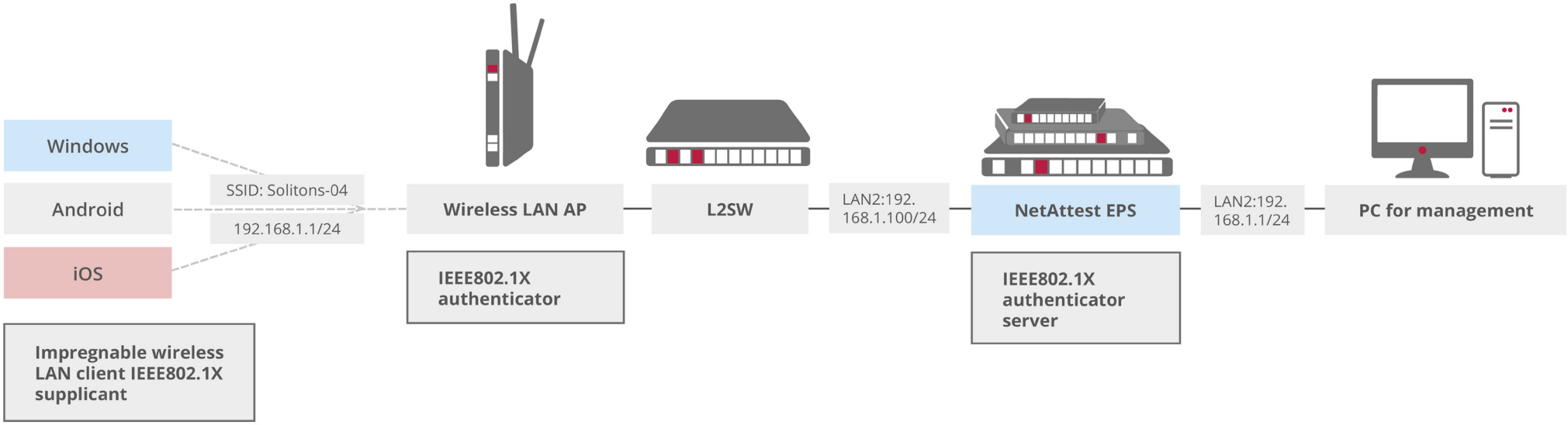


FIGURE: IEEE802.1X AUTHENTICATION CONFIGURATION

Components, protocols and authentication methods

These are the three main components of IEEE 802.1X authentication:

1. Authentication software on the client (device), by default provided in the OS

2. The access point that supports IEEE 802.1X authentication

3. The RADIUS (Remote Authentication Dial-In User Service) authentication server

The authentication protocol is EAP, and the main authentication methods are the following:

1. EAP-PEAP authentication using an ID and password

2. EAP-TLS authentication that uses an electronic certificate

A significant difference between these two authentication methods revolves around the digital certificate, which is only installed on the client in the case of EAP-TLS.The digital certificate is used on the server with both authentication methods.

The difference between EAP-PEAP and EAP-TLS

In the case of EAP-PEAP, an ID and password are used for authentication on the client side. An advantage is the easy setup required by the client.

However, anyone who knows the password can connect to the network from office PCs or their personal device. This situation isn't a big problem if you work in an environment where the internal network is only accessed from office PCs.

However, the rise of unmanaged and personal devices has added a new level of risk, as they can bring out internal information when they connect to the wireless LAN. If the ID and password are leaked or stolen, these credentials could be used for unauthorised access from an unknown person's device. Now, this can be mitigated by using a second factor to provide a higher level of proof. However, this can either prolong the user's login process or be easily bypassed by attackers through weaknesses in the 2FA implementation or by tricking the user into providing the second factor.

The Downside of EAP-TLS

The solution to the above mentioned problem lies in EAP-TLS. With this authentication method, a digital certificate is installed on the client to provide the highest level of proof. This approach also solves the risks of getting trapped by the infamous Man-in-the-Middle. Additionally, access from a PC or smartphone without such a digital certificate is rejected altogether.

Therefore, EAP-TLS gets you far stronger authentication than EAP-PEAP. There's one problem, though, as EAP-TLS comes with operational difficulties, such as distributing digital certificates to each client. It takes a lot of time and effort, so companies haven't widely adopted EAP-TLS. This is a shame, as the authentication method ensures robust security.

4. Building and operating an EAP-TLS system - 7 elements

In this chapter, we'll discuss the seven essential components needed to build and operate an EAP-TLS authentication system.

Operational difficulties put aside, what does it take to build and operate an EAP-TLS system? Here are the seven key elements:

1. LAN switch and access point that supports IEEE 802.1X
2. RADIUS authentication server
3. CA (certificate authority) server
4. DHCP server to issue correct IP addresses
5. System to distribute the certificates and link with the user database
6. System to back up information on each server
7. Procedures and expertise for designing, operating, and troubleshooting these systems

Establishing an authentication infrastructure for client authentication isn't too much work. However, you also need to set up a private CA, a link with the internal Active Directory (AD) or LDAP and build the system to distribute the certificates to clients and other methods to operate the authentication infrastructure properly. Sometimes, you must consider fault-tolerant design, management tools and whether the AD link is allowed. Then there are some basic considerations about the authentication server in the corporate system. Let's have a look at them next.

Concerns of scalability

Can the server be used for SSL-VPN authentication?
Authentication in the browser dedicated to business operations, single sign-on authentication, remote desktop authentication, and other authentications?

Can the authentication method be easily modified?
For example, can a one-time password be easily applied in addition to the certificate?

Considerations of multi-functional device support

Can the digital certificates be distributed to multiple OSs?

Concerns of operation workload

Can the digital certificates be quickly and safely distributed according to your environment?

Can users who haven't used the system for a certain period easily be organised?

Can the server be linked to the internal AD or ID management system?

Considerations of reliability

Can safe operation be realised?

How about the domestic support system?

5. NetAttest EPS: an all-in-one authentication appliance

To implement EAP-TLS authentication, you would need a lot of tools. To make it easier for you, Soliton developed NetAttest EPS: an all-in-one authentication appliance product that simplifies EAP-TLS. The solution provides answers to both security and operational challenges. After all, a quick and easy setup builds confidence in the IT department, and ease of use helps employees adopt a new way of working. Both are crucial factors when introducing a new tool.

NetAttest EPS includes the RADIUS authentication, private CA, certificate distribution and management functions. The greatest asset is the easy implementation and workability, as no special knowledge or technology is required. To illustrate this, let's compare the performance of NetAttest EPS to a "normal" implementation.

A 'normal' build an EAP-TLS-enabled authentication infrastructure:

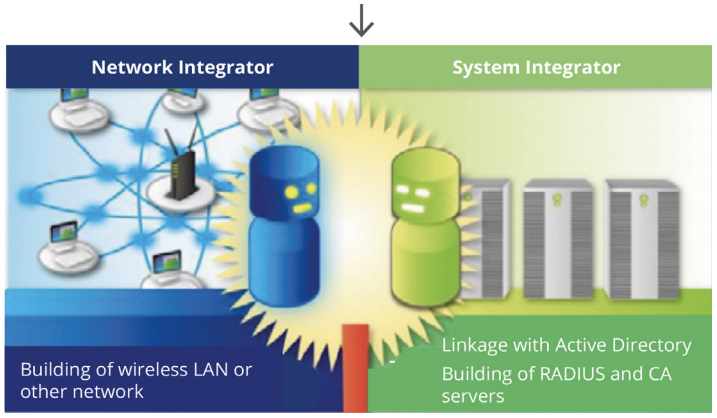
1. Preparation of hardware
2. Installation of OS
3. Building of private CA
4. Installation of RADIUS
5. Setup of RADIUS
6. Setup of users

With NetAttest EPS, we managed to reduce this process to three steps. But we didn't just decrease complexity: the required time is less than half.

How you build an EAP-TLS-enabled authentication infrastructure using NetAttest EPS:

1. Installation of NetAttest EPS
2. Initial setup wizard
3. Setup of users

Typical Case



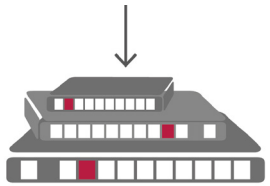
Difficulty of linkage

Coordination among staff and vertification of linkage

Separation at failure

Increase in processes and time

When using NetAttest EPS



Users without special knowledge can quickly build the environment.

Time saving explained

Generally, when building an IT security solution, network integrators are in charge of building the wireless LAN environment. System integrators, in turn, are in charge of the AD link, the RADIUS server, the CA server, and (often) other servers. This division of roles often causes delay, as integrators focus on their field of expertise. In contrast, they should understand both network integration and system integration to see the bigger picture and work together.

Therefore, we developed NetAttest EPS so that both network integrators and system integrators can take on every possible task, which speeds up the process. This approach results in a quick implementation that requires less specialised knowledge, making it less prone to error.

In addition, NetAttest EPS is an all-in-one product that provides all the functions needed to build an IEEE 802.1X authentication server. Think about components such as abundant RADIUS authentication functions, intuitive Web UI, easy AD link, a settings backup/restoration function, support for redundant configuration, and many proven records of linking with devices from Wi-Fi and VPN manufacturers. By implementing NetAttestEPS, you can easily implement a safe authentication infrastructure based on IEEE 802.1X.

6. Digital Certificates: the New Standard

In this chapter, we'll discuss why digital certificates are becoming the new standard for network authentication and security. You'll learn about the benefits of using digital certificates, how they work, and how they can be implemented in your organisation.

Digital certificate authentication is powerful because a different certificate is installed on each client. It ensures the robust security that's so highly needed for corporate wireless LAN. It's also what sets the method apart from insufficient security measures such as PSK (pre-shared key) authentication, where multiple users share the same password, or MAC address authentication.

But having said that, using a certificate doesn't always ensure robust security. For example, attackers can illegally obtain a certificate to spoof a legitimate device, depending on the distribution method. A certificate could be stolen and exploited when an outsider finds out and exploits the password. So, what needs to be done to raise the certificate security level? In the next section, you'll read how to identify and avoid hidden security holes when using certificates. We'll also introduce you to the functions of NetAttest EPS that will help you in this quest.

How Digital Certificates Work

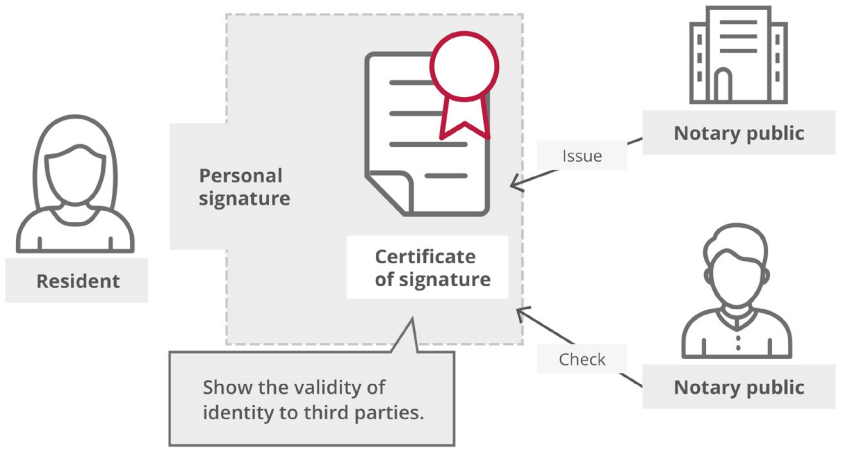
Many believe that certificate management is difficult and time-consuming, but it's not hard once you understand the mechanism.

A digital certificate is an electronic file that proves the identity and other properties by applying public key encryption. Public key encryption needs both a private key and a public key and uses a security infrastructure called PKI (public key infrastructure) to validate (authenticate) identity.

You can think of the private key as your signature and the public key as the "certificate of authenticity". If you pair your signature with a certificate from a notary public or other organisation, then you really have something. The same applies to electronic security certificates. With PKI, each user has a private key ("signature") to prove their identity. In addition, the user gets a public key (certificate of authenticity) from the certificate authority ("notary public"), dispelling any doubt.

Together, the private key and public key form a strong combination. Data can only be decrypted using the paired key; the servers that manage the user's device and certificate exchange this key pair between them for actual authentication.

Example



PKI (Public Key Infrastructure)

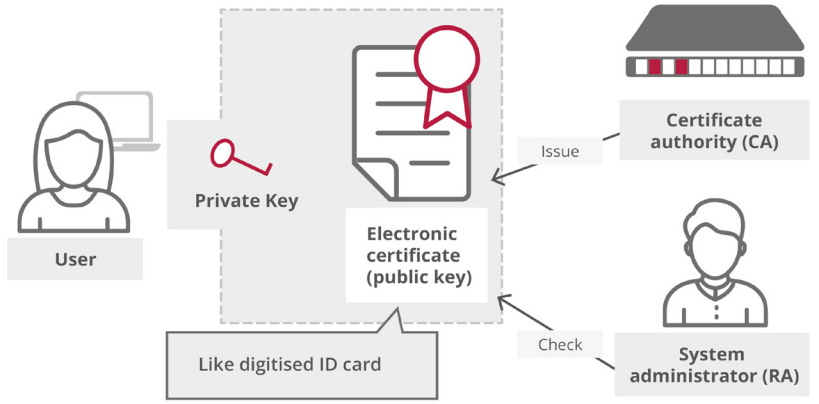


FIGURE: IEEE802.1X AUTHENTICATION CONFIGURATION

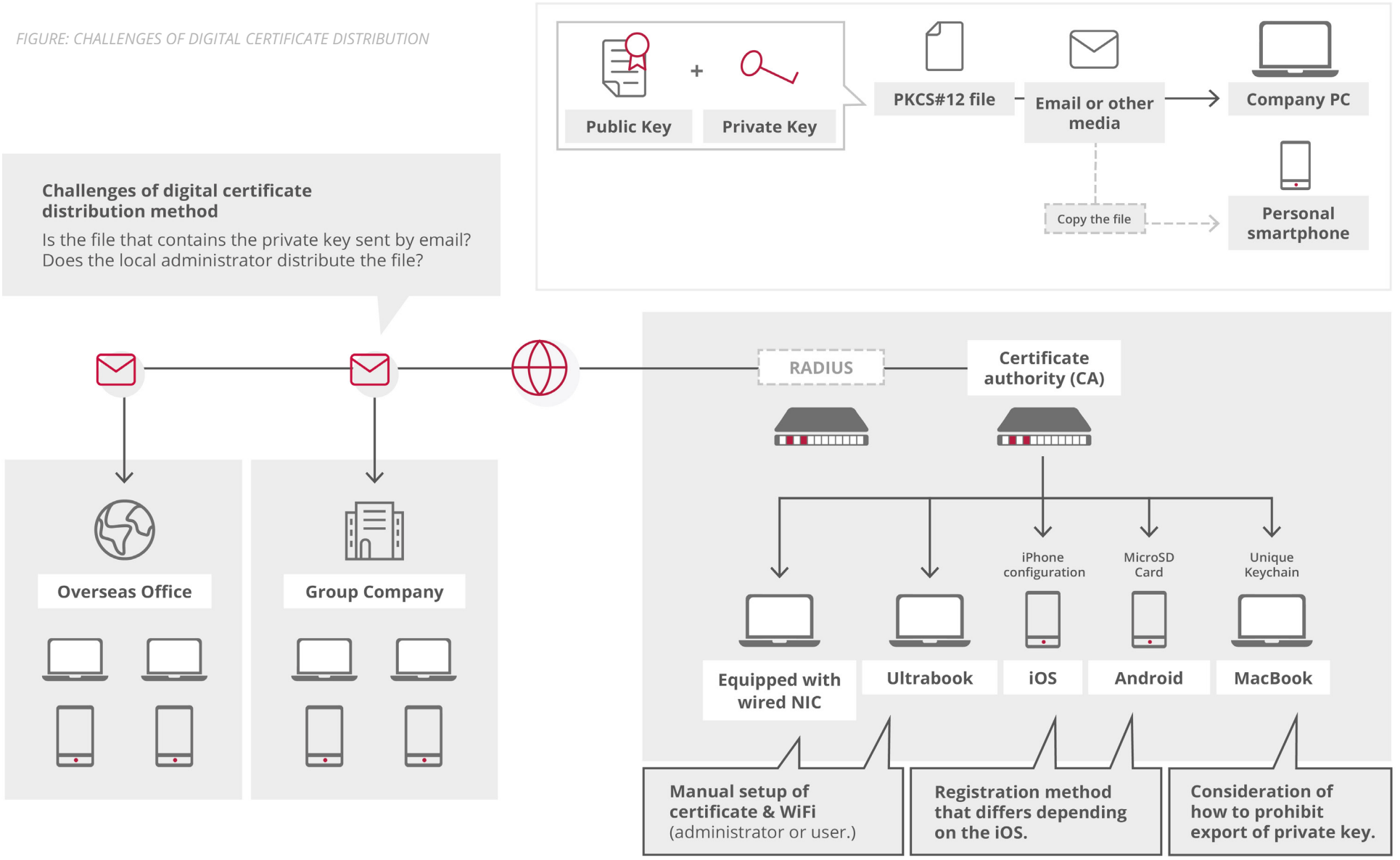
Impersonation: The Hidden Security Hole in Certificate Distribution

To use this public key encryption method, you must first install the public key (certificate) and private key on the user's device. As you're probably familiar with Internet banking or administrative services using electronic certificates, you'll understand that safe communication cannot be established without importing public and private keys into the client's PC.

This importing is done with a PKCS#12 file, which is used to import the certificate into the client's PC. The PKCS#12 file contains both a public key (certificate) and a private key that form a pair. The problem is that the PKCS#12 file can be copied. In addition, if it's allowed to export the private key, it can also be copied.

In other words, if the certificate is distributed via email or other media, a malicious person who obtains that email can easily make an illegal copy. This situation allows intruders to impersonate an authorised person and is, therefore, an important security hole in certificate distribution.

FIGURE: CHALLENGES OF DIGITAL CERTIFICATE DISTRIBUTION



The chances of intruders stealing your certificates may seem small, but in a recent Internet banking case, the attacker acquired the private key in three easy steps:

- The user asked the bank to reissue the certificate.
- A malicious program copied the certificate when the user imported the reissued certificate.
- The attacker sent the copied certificate to their server instead of the user.

This attack targeted an unguarded point while the user felt safe as he had prohibited the export of the private key. This illustrates the insufficiency of reactive measures, as they're powerless to protect against increasingly advanced cyberattacks.

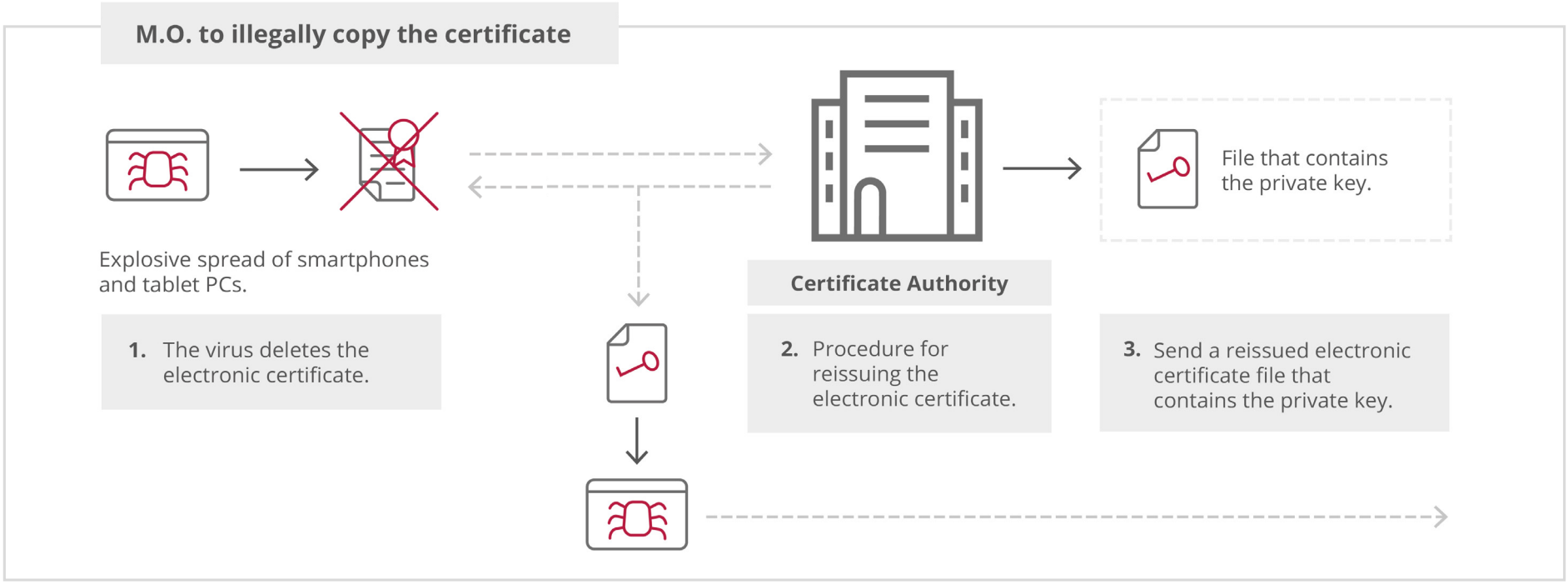


FIGURE: THERE'S A RISK ASSOCIATED WITH ISSUING A CERTIFICATE USING A FILE THAT CONTAINS THE PRIVATE KEY

In an ideal world, you would implement an EAP-TLS-enabled authentication infrastructure that's free from all of the security holes mentioned above. This isn't easy, as cyberattacks get more sophisticated every day. And as the following example illustrates, you can't fundamentally eliminate attacks simply by prohibiting the export of private keys. NetAttest EPS doesn't use the PKCS#12 file to import the private key to address this situation.

Instead, the user's client device generates the private key itself and never leaves the device by any communication path. That's a large problem solved!

Certificates can only be generated and distributed in a closed network environment such as LAN when the private key and the public key are imported to the user's device. Automate certificate distribution and settings with PCs and multi-functional devices using iOS, Android, or Mac OS.

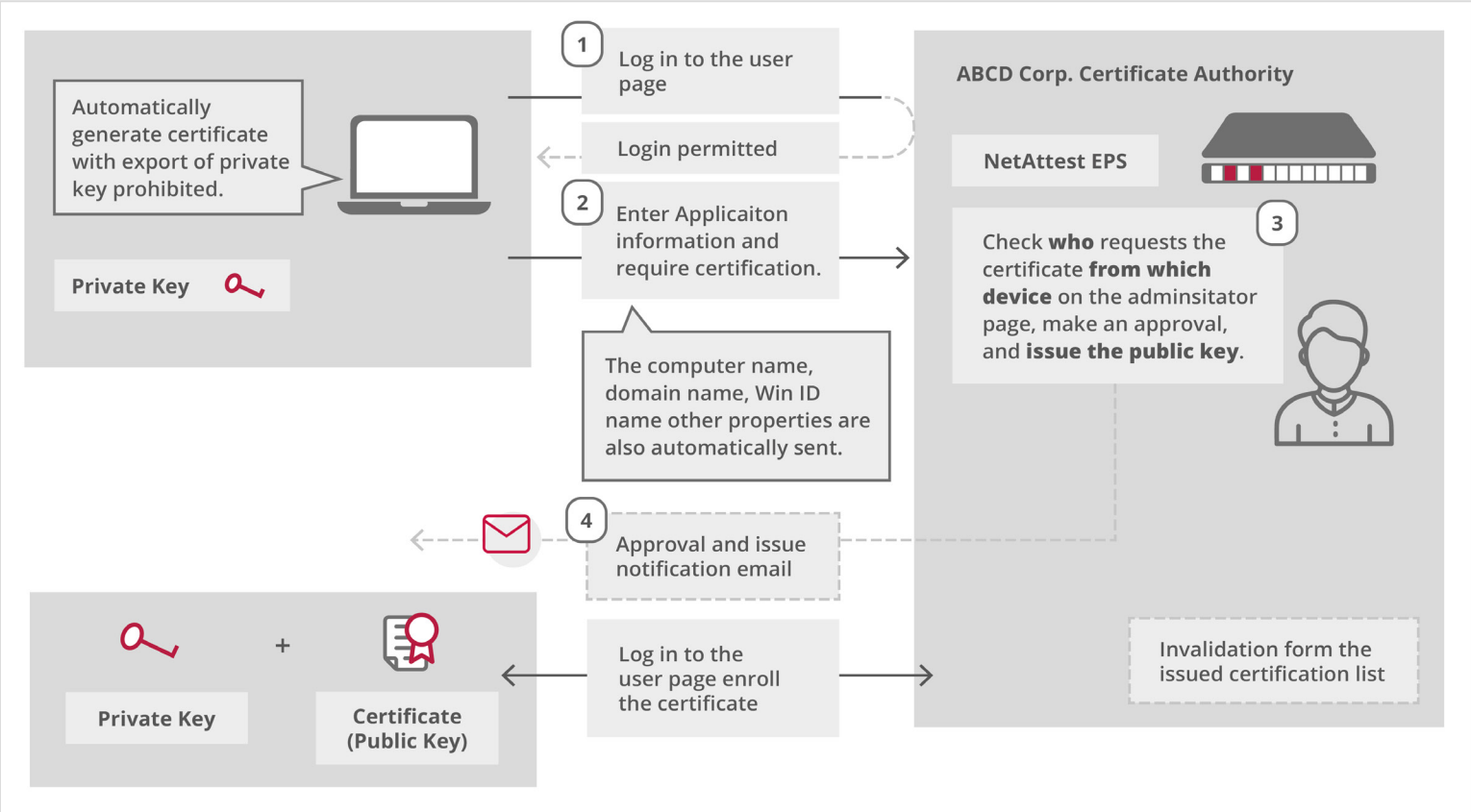


FIGURE: : ISSUE OF CERTIFICATE IN NETATTEST EPS WHERE A FILE CONTAINING THE PRIVATE KEY IS NOT USED

7. How to save time and improve network security without sacrificing convenience

Network administrators and IT departments often see authentication as a burden. NetAttest EPS changes that perception. Quickly implement Network Access Control and provide users with the most convenient solution on any device or operating system.

NetAttest EPS is a complete, port-based network access solution that uses the IEEE 802.1X standard as an authentication and authorisation server.

It's ideal for protecting both large and small networks, in one location or many, and it protects the wired, Wi-Fi and VPN. If you're tired of complex network access management and concerned about security, learn how NetAttest EPS will help you.

CASE STUDY:
Enabling easy and secure network access control as standard

A leading automotive supply chain manufacturer wanted to upgrade its network security and secure access via wired, Wi-Fi and VPN connections. The company needed to protect the network from growing threats, including ransomware from untrusted devices, and ensure they could be TISAX compliant — vital for any supplier, OEMs and partners contributing to the automotive supply chain in Germany.

The company's team collaborated with a partner to choose a Sophos security solution, but they soon realised that the solution lacked two vital components: Network Access Control and certificate management. These elements were crucial to comply with TISAX and ensure sufficient network protection.

Due to the connection of business-critical production machines to the company's network, any potential network threats could spread to these devices. To mitigate this risk, Soliton recommended network segmentation to protect the production machines from intrusion. By isolating threats to one part of the network, the risk of spreading throughout the entire organisation is minimised.

The Results: Smooth Operations for 3+ Years

The implementation began with a POC, which was later validated, and the transition to the live environment was quick and straightforward, taking place during a lunch break. The NAC solution has been running smoothly for over three years since its implementation, benefiting both IT and end-users. Certificate renewals are painless, and users receive an email reminding them to renew. If they still have network access rights, they receive a new certificate. Additionally, the solution is low-maintenance for IT, and the robust implementation has ensured smooth operation since its deployment in the production environment.

Why Choose the NetAttest EPS NAC solution?

Network administrators often see access control as a burden. NetAttest EPS changes that perception, making it easy to implement network access control and provide users with the most convenient solution on any device or operating system.

NetAttest EPS is a complete, port-based network access solution and uses the IEEE 802.1X standard with EAP-TLS to act as an authentication and authorisation server. It's ideal for protecting large and smaller networks in one location or many, protecting the wired, Wi-Fi and VPN network access.

Would you like to know more about NetAttest EPS? Schedule a meeting with one of our IT security experts below!

Schedule A Meeting

EMEA Office

Soliton Systems Europe N.V.

Barbara Strozzilaan 364 | 1083 HN
Amsterdam | The Netherlands

+31 (0)20 896 5841
emea@solitonsystems.com
www.solitonsystems.com