Security Whitepaper

Legal notice

This document is intended to answer questions such as "How does AnyDesk help to make sure that my session is secured?" Particularly AnyDesk's operational security processes are described for the network and server infrastructure.

AnyDesk Software GmbH
Friedrichstraße 9
70174 Stuttgart, Germany

Managing Directors/Geschäftsführer: Ph. Weiser, A. Mähler
Company Register/Handelsregister: Amtsgericht Stuttgart - HRB 748838
VAT-ID/Umsatzsteuer-ID: DE 294776378

Notices

This document is for informational purposes. It represents Any Desk' s current product and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AnyDesk' s products or services. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AnyDesk, its affiliates, suppliers or licensors. The responsibilities and liabilities of AnyDesk to its customers is controlled by agreements, and this document is not part of, nor does it modify, any agreement between AnyDesk and its customers.

AnyDesk is designed to be connected to and to communicate via a network interface. Customer shall establish and maintain any appropriate measures (such as but not limited to the application of authentication measures, encryption of data, etc.) to protect the product, the network, its system and the interface against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information. AnyDesk is not liable for damages and/or losses related to such security breaches, any unauthorized access, interference, intrusion, leakage and/or theft of data or information.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art security concept. AnyDesk' provides such concept. You are responsible for preventing unauthorized access to your systems, machines and networks which should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information, please contact visit https://anydesk.com. AnyDesk recommends applying updates and to use the latest available version. Use of versions that are no longer supported, and failure to apply the latest updates may increase your exposure to cyber threats.

Contents

AnyDesk Security Architecture

Introduction

AnyDesk' s security architecture is built on TLS 1.2 as a standardized protocol. Using a well-known and publicly reviewed protocol helps us to avoid many of the common pitfalls that occur, when people try to build their own cryptographic protocols. Using TLS also makes it easier to update ciphers or to mitigate vulnerabilities that might be discovered by researchers.

All the information in this document applies to the latest AnyDesk version. Older versions may use older and less secure algorithms or protocols.

This documentation applies to the server system operated by AnyDesk itself (the "live system") and to the On-Premises solution.

Server connection

AnyDesk keeps a persistent and encrypted connection to one of the AnyDesk servers, while it is running. This connection will be established through port 443, 80 or 6568, depending on which connection is successful first. This allows the server to contact the client in case of an incoming session. The connection is secured using TLS 1.2.

The key exchange on the AnyDesk live system is performed using ECDHE[1] with a 256-bit ECC[2] certificate. The on-premises solution uses a DHE[3] key exchange with a 4096-bit RSA certificate. Both methods provide perfect forward secrecy. The actual encryption of the data stream will then use 256-bit AES encryption in GCM[4] operation mode.

Authentication of the Server

The AnyDesk servers are authenticated through TLS, using their certificate. For this purpose, we have established a Root CA for the AnyDesk server system, that is explicitly trusted by the AnyDesk client software. Every server in our system has a certificate that is signed by that Root CA.

For the On-Premises solution, a certificate for the Root CA and a server certificate signed by that CA are generated during the installation process. Both are 4096-bit RSA certificates. The Root CA certificate is uploaded to my.anydesk.com, to generate a customized AnyDesk client version that explicitly trusts the Root CA of this server.

[1] Elliptic Curve Diffie-Hellman Ephemeral
[2] Elliptic Curve Cryptography
[3] Diffie-Hellman Ephemeral
[4] Galois/Counter Mode

Authentication of the Client

When starting AnyDesk for the first time, the client will generate an additional self-signed 2048-bit RSA certificate that will be used to identify the client itself to the server (the "client certificate"). This client certificate is communicated to the server during the TLS handshake using TLS client authentication.

When the client connects to the server for the first time, the server will allocate an AnyDesk Client-ID and permanently link it to the client certificate's fingerprint. On subsequent logins the server will identify the client again based on this certificate fingerprint. This ensures that a Client-ID can only be impersonated if the private key for the client certificate is known.

Client to Client connections

When requesting a session between two clients, AnyDesk will use the server to orchestrate that connection as well as using the server as the authority to authenticate the clients. The server provides the clients with the information required to establish a direct connection and will also send them the respective client certificate fingerprints.

The clients will then try to establish a direct TCP-connection between them and secure it via TLS. During that TLS handshake, both clients will identify themselves with their client certificates and verify that information against the fingerprints provided by the server. This ensures that the Client-ID cannot be impersonated without knowledge of the private key.

The key exchange will be done using a DHE key exchange, providing perfect forward secrecy. After that the connection will be secured using 256-bit AES in GCM operation mode.

If a direct connection cannot be established, the session data will be exchanged over the secure server connection that have already been established.

Deprecating Certificates

In the event that the server certificate on the On-Premises solution is compromised, both the Root CA and server certificate must be regenerated on the server. This prevents existing AnyDesk clients from connecting to the server. A new customized client must be generated in my.anydesk.com followed by a new roll out. Existing clients will then have to be replaced by that new AnyDesk client.

TLS Interception

Using a Firewall with TLS interception is generally not possible with AnyDesk. We advise users to selectively disable the TLS interception for AnyDesk in their firewall. The reasons for this are:

AnyDesk uses TLS client-authentication to identify the AnyDesk client to the server. A firewall performing TLS interception won't have access to the clients' private key and will thus be unable to perform the client authentication.

The AnyDesk client software does not use the Operating Systems certificate store to validate the server certificate, but only explicitly trusts the AnyDesk Root CA and certificates (the server certificate) signed by it.

Therefore, the AnyDesk client will not trust the certificate generated by the firewall and reject the connection.

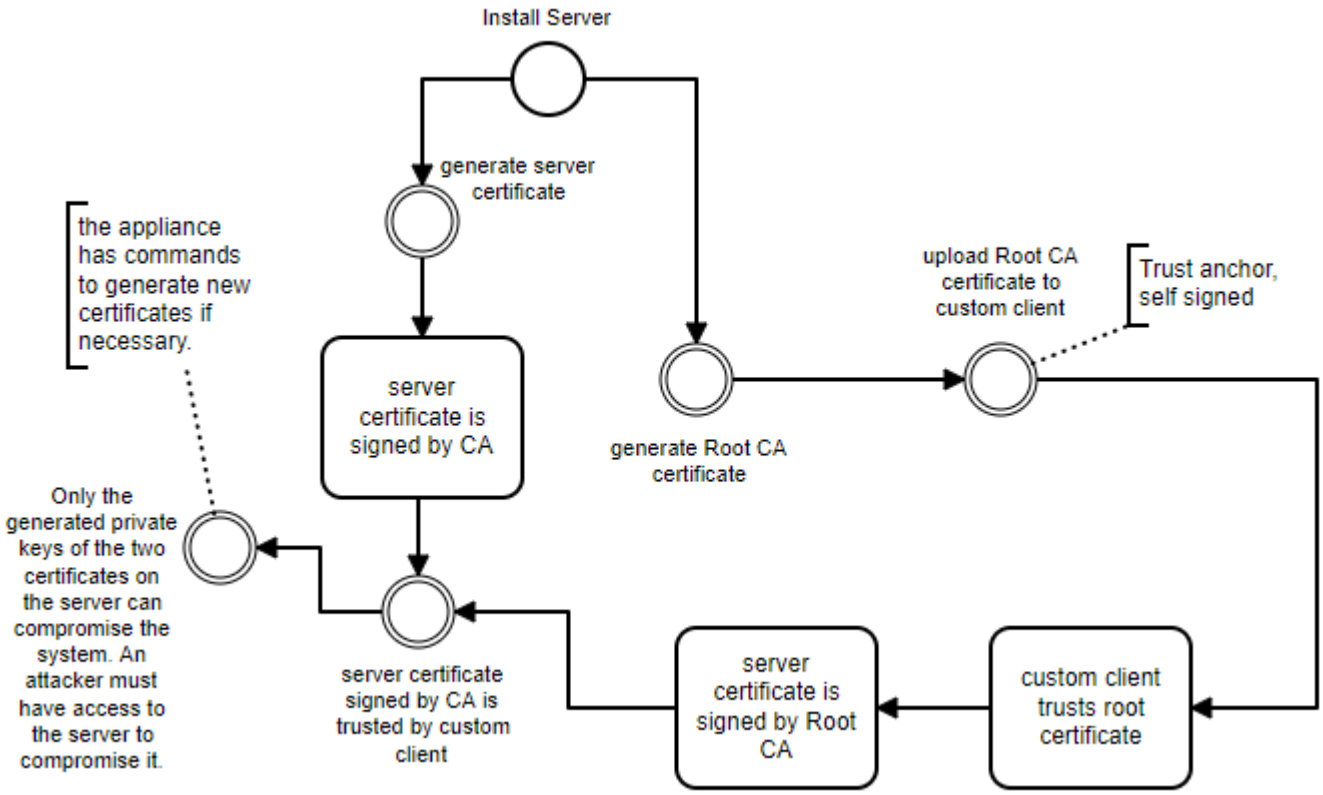
AnyDesk is not using HTTPS but uses a proprietary protocol over TLS. Therefore, even if the firewall would be able to perform the TLS interception, the level of protection that the firewall could offer would be severely limited, because the firewall would be unable to decode our protocol.

TLS was not designed with interception in mind and we believe that performing TLS interception, which is essentially a man-in-the-middle attack weakening the security of the system and increase the potential attack surface.

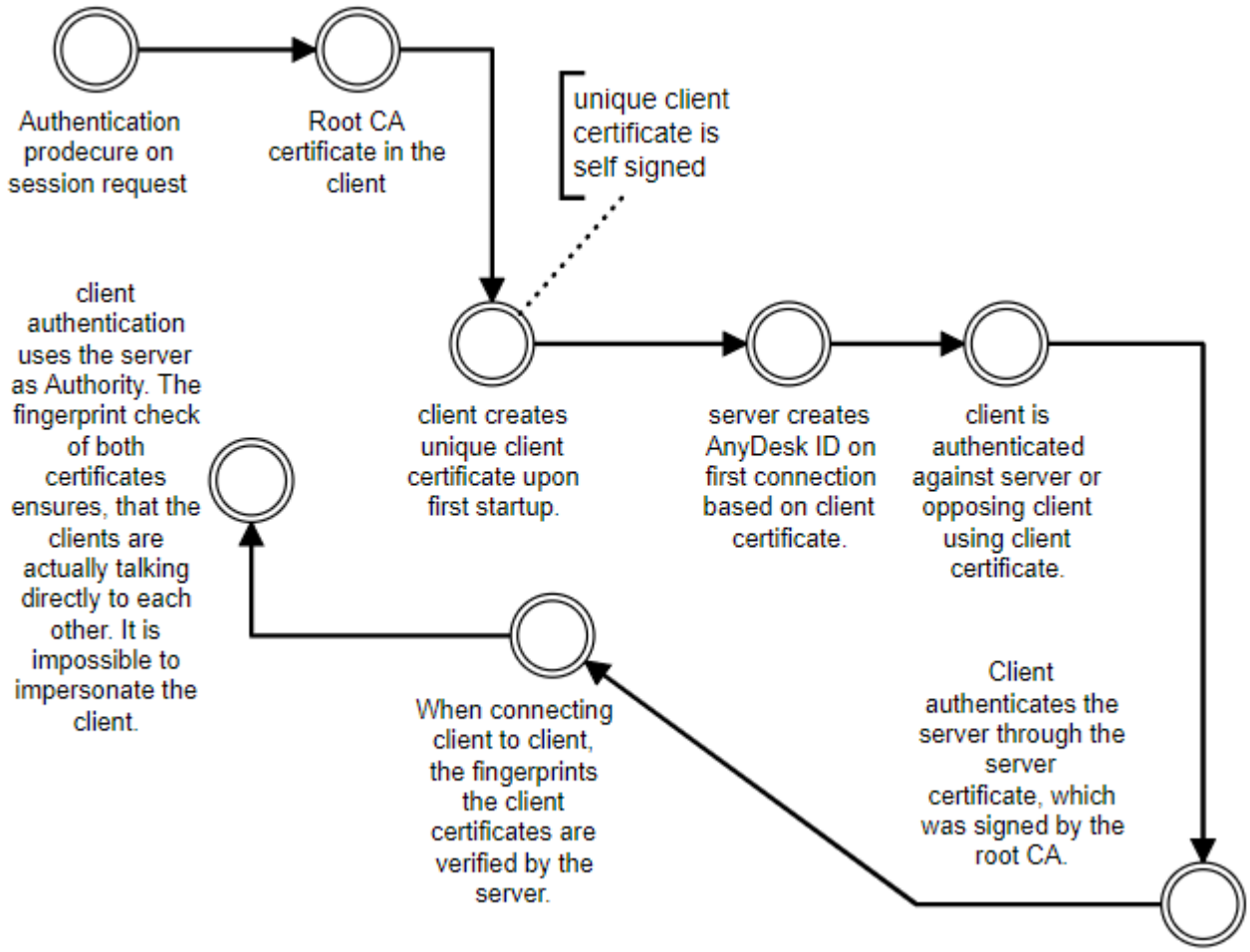
Server Setup

- create Root CA certificate
- create server certificate
- sign server certificate by root CA
- upload root CA to my.anydesk.com
- custom client is hardcoded with root CA and IP/DNS of OnPremises Server
- client-based TLS authentication / client only trusts the server certificate.
- server is authenticated by the client using root CA.
- client to client connection is authenticated against each other using server as authority by validating fingerprints of each other' s unique client certificate.
- No mechanism of revoking certificates. (Not applicable for this setup)
  In the unlikely case of compromising the private keys of either certificates which can only happen when the server itself is compromised, new certificates must be generated using generate command (See Manual)

  The former certificates are thereby replaced and therefore revoked. This action required another roll out of the custom client.



Session Authentication Procedure



Encryption

client-server connection: ECDHE-RSA-AES256-GCM-SHA384
client to client connection: DHE-RSA-AES256-GCM-SHA384

Both Ciphers are based on DHE-handshake and provide perfect forward secrecy.