



Secure Web Conferencing

Table of Contents

3 UTIMACO – your trusted partner

Secure Web Conferencing During the Pandemic and Beyond

4 Where life gets blurry – adjust your focus

Build on a trust anchor that allows to **protect and control** your own data

5 At a glance

12 recommendations to foster a security conscious evaluation of web conferencing solutions:

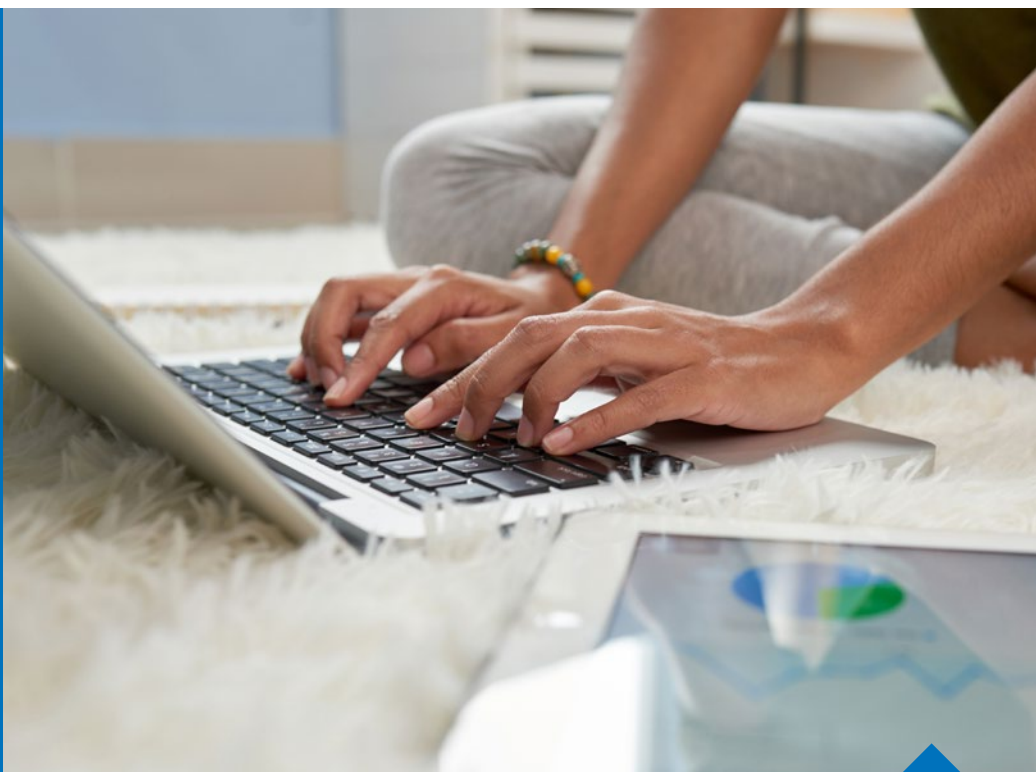
11 UTIMACO Solution Portfolio

The most versatile Cyber Security offering



UTIMACO – your trusted partner

At Utimaco, we develop hardware-based encryption and key management solutions that provide the highest level of security and assurance. Over the last 35 years we have put together a broad portfolio to address requirements to web conferencing systems as defined by NIST and German BSI. Our solutions are centered around cryptography, secure key management as well as data encryption with a variety of auditing options – certified and read-to-use.



We are trusted by Fortune 500 companies who deploy our solutions to embed security in their own products and services – in the cloud and beyond.

Utimaco provides you with a trust-anchor at the flexibility of your needs through a mix of integrated hardware and software solutions.

However, solutions are only as good as the people who know them – thus, we are very proud of the people who build, manage and maintain our solutions. We would like to share our enthusiasm and passion with you, and would be delighted to provide you with consultancy, training and support to get you ready for tomorrow's challenges.

We can offer your organization the following benefits

A comprehensive Post-Quantum Cryptography and Blockchain toolkit

The most flexible Crypto SDK in the market, which will enable your team to tailor the use of our hardware encryption product suite to your specific needs.

A path to rapidly start testing and integrating our Hardware Security Modules (HSM) in your product suite, through the use of our [HSM Simulator](#), which can be downloaded for free

A turn-key solution for full key life-cycle management, auditing and role-based access

Hardware-level encryption with the highest level of certifications including FIPS 140-2 Level 3 & 4 and CC EAL4+

Where life gets blurry...

This quote has never been more relevant with regards to IT systems. In a world where data travels between continents, gets processed on a plethora of different systems, stored on a variety of different media and can be shared with a countless number of individuals – in just a second – control over your own data should be more than just a bit of wishful thinking, about how ‘wouldn’t it be nice if...’.



We strongly believe that it is in everyone's interest to have a trust anchor, that allows them all, individually, to **protect and control** their own data. The core of UTIMACO's business is providing the hardware and software necessary to implement these trust anchors. Correctly implemented, hardware-based trust anchors can mitigate risk, and lessen liability, when viewed through the lenses of these regulations.

...adjust your focus

When using web conferencing software, the user is presented with several options to secure and protect a scheduled meeting. These settings provide different qualities of service (QoS), but QoS is a playing field where changing one setting may have unexpected, diverse and hidden effects elsewhere. However, there is always more than just the things presented to the user in the application interface.

Web conferencing systems make use of cryptography in the background, store data on different systems, media and locations, forward that data to different, authenticated users, send (hopefully authentic) meeting invitations or even automatically analyze your call to create transcriptions. The list of options has heavy impacts on your data confidentiality, integrity and authenticity.

The following
12 recommendations
provide a starter package
to foster a security
conscious evaluation
of web conferencing
solutions.

At a glance

01 Randomness

The quality of randomness is important for any feature and capability that relies on random – not just the “non-functional” issues like having visible random meeting IDs and passwords.

These meetings rely on cryptography to protect each and every session, and cryptographic operations need truly random keys for the steps that are frequently, and silently, invoked before, during and after each meeting.

Examples are

- Randomly generated meeting-level session keys for transport encryption.
- Key agreement protocols (Diffie-Hellman, etc) can be used to establish true, end-to-end encryption between clients, ensuring confidentiality, integrity and authenticity protection of user data (personal profile, billing information, ...), recordings, session content (recordings, chat messages, shared files, system logs and configuration data)
- Role based access and authentication controls for login to the conference platform, but also authenticating legitimate staff (administrators, auditors, ...)

Protect
your call with an
(ideally truly random)
Meeting-ID and
password

02 Data Stores

To build a convenient and feature-rich system personal data is maintained for each user (name, email address, billing information, personal preferences, etc.), but also session recordings and shared files must be stored – somewhere, and somehow.

Storing user data (including any recordings, chat logs, etc) carries with it liability, according to laws and regulations such as the [General Data Protection Regulation \(GDPR\)](#) and California's CPAA consumer protection act. However, some requirements may, in certain jurisdictions, be superseded by other regulations – specifically those dealing with lawful inspection (e.g. [US Cloud Act](#) vs GDPR). Where the data is stored – even transitionally – determines under what jurisdictional “lawful inspection” regulations apply. Access to the data passing through a server is controlled by the laws of the jurisdiction in which that server finds itself.

Additionally, data assurance around sensitive data should not only be concerned with obviously personal data, but also user or meeting metadata: Even event signals (incoming call, meeting has started, ...), logs, participant information, etc should be protected to comply with the law and provide a maximum level of data security. Consequently, unprotected data must be reduced to a minimum, and this leads to the requirement for true end-to-end protection (encryption and authenticity) at least for session streams, but also ideally for any shared data.

It's
paramount
that the provider offers
a choice (and guarantee)
where company and user
data will be stored
or routed.

Manipulation and tampering of data must be detected and signaled in a safe, unfalsifiable way, one that is itself not subject to manipulation or tampering.

Finally, access to all data has to be restricted – reliable means for authorization (proper authentication in combination with e.g. policy-based access permissions) have to be put in place and shall be logged.

Web
conferencing
is much more than
just the session
itself.

Keep an eye
on where and how
your data is stored –
but also who has
access to it

03 Cryptography

Cryptography – used in the right way – is a building block to fulfill key principles of information security:

- **Confidentiality**
that which I send, is only comprehensible to you
- **Integrity**
that which I send, is what you received
- **Availability**
that which I send, is available to you and only to you based on role or specific policy
- **Non-repudiation**
it is provable that what I sent to you, was sent by me (and I can not claim otherwise)

Applying crypto in the correct way is just the start. It's also important to check for the algorithm and key size choices, and the way how they are used. Bear in mind that some data will be stored for decades (e.g. on backup tapes) so the choice of cryptographic techniques also needs to account for long-term security.

Finally, locks are only useful if the key is stored (and managed) carefully – or, locks are only designed to keep honest people honest. Secure key storage goes hand in hand with secure key management, life-cycle planning and strict access controls. Depending on the sensitivity (from “useless and no risk related to disclosure after a short-term period”, to “absolute requirement for long term security guarantees”) and lifetime of data (data stored or data being flushed/wiped after the session) different approaches of key vaulting and deployment have to be considered.

A key management system can significantly reduce the dangers of oversights, misconception and missing auditability.

Evaluate the crypto being used

“ A basic understanding from a helicopter view is necessary to spot potentially vulnerable parts of the service, to enable corrective action. ”

04 Architecture

It's an illusion to expect that every component of the system architecture, as well as the interactions of these components, can be understood in-depth, which emphasizes the need for strong end-to-end protection of data. Encrypted data is good, un-shared encrypted data is even better...

For those components that need to process sensitive data, it's important that access to that data be limited to the absolute minimum required to provide the service.

These components, and their interactions, need to be identified and thoroughly checked for encryption endpoints, meaning components that will decrypt the data. And, importantly, these components will themselves require special protection, e.g. two-factor authentication, system hardening and encryption, even the use of dual-access control may be necessary.

Furthermore, an assessment must be done to determine if at least some of these critical components can – or should – be hosted on-premise.



05 Management

As a very basic requirement, a web conferencing solution should enable you to control access to the system (e.g. login). It should also provide the meeting host with means to control who's attending, who should be excluded from a meeting and who should be able to present, gain mouse and keyboard control or mute/unmute participants, restrict the use of web cams and manage virtual waiting rooms to prevent unauthorized meeting attendance.

If the system includes ready-to-use physical devices such as e.g. conference room systems, the access to these systems should be restrictable as well – a SIEM integration of these devices deems also to be beneficial.

From an administrative point of view things like built-in and automated patch management, enterprise grade user management (e.g. built-in AD/LDAP, SAML, OpenID Connect, SSO, ...) or at least a centralized management help to reduce risks such as orphaned or rogue accounts. This requirement goes hand in hand with role-based access controls.

Control also means controlling key material. Keys should be manageable and the access restricted. Features like full key life-cycle planning assist in reducing risks related to compromised keys. As a benefit, key control can also be leveraged to fulfill requirements for data retirement (right to be forgotten) – a key once erased and not recoverable immediately renders data encrypted with it useless (with one major caveat: data stored decrypted remains unaffected).

It depends on the definition of control and the control of what?

Who is in control?



06 Authentication and Authorization

To be able to see a list of participants, and an option to exclude – and block – attendees from meetings is essential.

To enhance security, options to use two factor authentication and/or digital identities (Certificates, OpenID Connect, Kerberos, ...) for entity authentication should be considered. This requires that there be a way to establish trust between the web conferencing system and an entity, to provide a way for a trust relationship to be established (e.g. PKI infrastructure with strong trust anchors) and it is of utmost importance that the assets used for this trust relationship be themselves protected – in most cases that means protecting digital keys in hardware-based devices.

Sharing these digital identities between different devices (e.g. laptop and mobile) and thus protecting them in different environments with different (hardware) capabilities requires a well-designed concept.

A different problem is how to use a digital identity if participants dial-in in a traditional way – e.g. [one time passwords \(OTP\)](#) have proven to be an adequate choice.

Lastly, secure authorization is not just limited to participants of a meeting, but also includes operative and administrative staff of the web conferencing system. Employees and systems of the provider should not have access to the meetings or the meeting recordings, except via explicit permission provided by the end-user (e.g., for support purposes), or due to lawful inspection requirements. Data, and metadata, should not be available to unauthorized, nor unauthenticated, entities.

Once established, secure authorization mechanisms can also provide additional benefit, e.g. granting access to data (shared files) or obtaining permission to store and process data (storing recordings and/or shared files, automated creation of transcripts, ...).

Who am I, and if needed, how many?

In the majority of cases, a web meeting is something very personal, and will contain sensitive information – corporate or individual. Access by unauthorized persons should not be allowed.

07 User Interface

How hard is it to get things wrong?

The majority of users will never use more than the user interface to login, schedule calls and set controls during a running session. The UI should be intuitive, clear and hard to get wrong while at the same time present the controls that are needed: Chat, whiteboard, attendee list, etc. Also important and useful is in-meeting signaling, ie the arrival or exit of attendees, changes to any currently applied encryption policy, usage of microphone, video and screen sharing, sharing of controls (mouse, keyboard) and start/end of recordings or data processing (e.g. an AI automatically transcribing the spoken word).

As to controls the host should, for security reasons, be able to lock sessions after the arrival of attendees, exclude attendees from a running session (entirely, or via use of virtual waiting rooms) and end the meeting for all participants.

Once a session has ended, the application should flush all remaining, session-related data.

When scheduling a meeting, the policy should be secure-by-default. At the minimum, this should include and require:

- New, randomly generated session IDs,
- New, randomly generated password
- Host-provided list of attendees
- Virtual waiting room (which the host must manually disable, if desired, once the meeting is started)

Virtual backgrounds and the option to limit controls for attendees (e.g. ability to unmute themselves or require requesting screen sharing permission) have turned out to be very useful functions that significantly increase security.



08 Quality

Regular software audits, and vulnerability testing are aspects which can be assessed without access to source code.

The most basic requirement is flawless functionality and best practice deployment. This includes aspects like patched third-party libraries (no outdated libs), no unnecessary and unprotected ports and services, digitally signed software (code signing) to guarantee authenticity and prevent client systems from running versions which have had malware added to them.

In addition, the software should apply the best possible security options to protect its data (user data, program data, binaries, ...). Other runtime options, e.g. support for [Address space layout randomization \(ASLR\)](#), provide additional boundaries against attacks.

Quality of Service and Software

“ While certain aspects of assessing software quality are hard to achieve without access to source code, others are not. ”

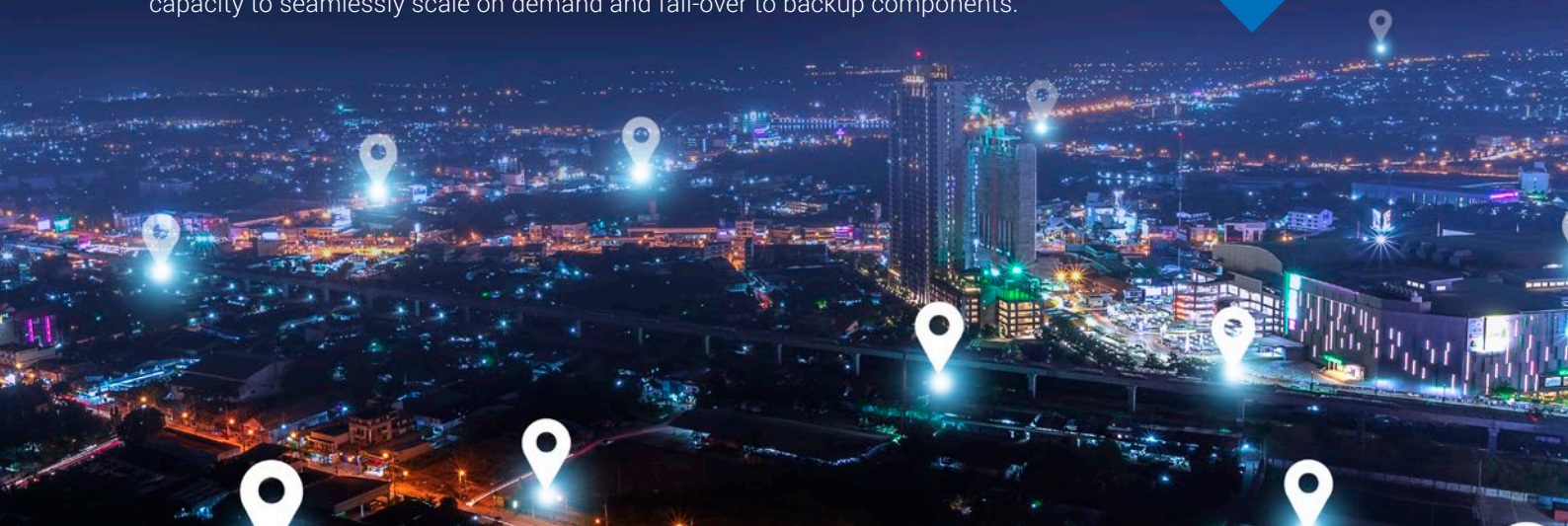
09 Availability

Publicly accessible (and up-to-date) up-time and system health data help to confirm vendor claims on availability. Business continuity and disaster recovery (BC/DR) plans should be available on request and include the full system with all of its components, and the BC/DR must include a policy for testing the BC/DR procedures, to ensure that it is full and complete, and that it encompasses all necessary requirements for continuity and recover.

Properly designed system components, and a proper recovery procedure, help to reduce down time and availability. The system should – in any case – provide enough capacity to seamlessly scale on demand and fail-over to backup components.

Reliability
is key

“Availability
is crucial to
business-critical
applications – meeting
break ups and significant
down time impact
day to day
business.”



10 Auditing and Monitoring

Auditability and monitoring capabilities (e.g. number of active users, meetings, quality of service, etc.) provide a big benefit not only to track appropriate licensing (e.g. providing enough licenses for all active users, scale on demand) and spot system issues – it is also essential to provide authentic information on system use and misuse (logins from unexpected locations), attacks (brute-forcing passwords), as well as GDPR related concerns such as obtaining permissions and access to e.g. key material and data.

In any case, appropriate authorization (role-base access, two factor authentication, ...) and data protection mechanisms (encrypting, digital signing, federated ledgers – block chains, ...) should be applied and in turn report their actions into the monitoring and auditing systems as well.



Big
brother
shouldn't be
watching
you

Monitoring should be provided by a centralized system hosted by the web conference provider, but it may also be supplied via an on-premise solution which receives monitoring data from the vendor or from client instances.

This same applies to audit data.



11 Data Privacy

Appropriate measures for data protection include the full range of information security solutions: storage-/file-/database/in-app-encryption, data authentication, tokenization, as well as entity authentication and authorization.

In short, cryptography is one of the fundamental building blocks and is an inextricable requirement for securing key material.

Say
GDPR,
one more
time...

“ Separating
keys from data
is a very useful measure
to significantly increase the
complexity required
for potential
attacks. ”

12 Certifications

Therefore, certifications should be looked at as a way to establish trust of the underlying systems – given the correct things have been evaluated (for an introduction to certifications, please refer to our [website](#)) – the deployed artifacts benefit from a certified and secure trust anchor, upon which they rely. Certify the wider view, within which the narrower products operate.

For cryptographic hard- and software [FIPS 140-2 / 140-3](#) levels and [Common Criteria](#) protection profiles and certifications are (among others) the most common types.

Again, it's important to check what has been certified and to make sure that the web conference provider runs the hard-/software at the certified patch level and in an appropriate mode (if applicable).

Take
a closer
look

“ It's
nearly impossible to
evaluate all components
of a web conferencing
system on your
own. ”



UTIMACO Solution Portfolio

The most versatile
Cyber Security offering



utimaco[®]

Root of trust
FIPS 140-2 Level 3 and 4

CryptoServer

- TimeStampServer
- Block-Safe
- Q-Safe

Atalla AT1000 PaymentServer

- Fast payment HSM
- Real multi tenancy

KeyBridge EKMS

- Payment Key Management

ESKM

- Enterprise Key Management

KeyBridge TokenBridge

- Tokenization

KeyBridge Pol

- Enterprise Key Management

DiscEncrypt

- Data-at-rest encryption

u.trust Anchor


- Supports multiple use-cases
- Cloud by design
- Containerized HSM



Get in Touch

in

UTIMACO GmbH

 Germanusstraße 4
52080 Aachen, Germany

 +49 241 1696-0

 info@UTIMACO.com

utimaco.com

utimaco[®]

© UTIMACO GmbH 05/20

UTIMACO[®] is a trademark of UTIMACO GmbH. All other named Trademarks are Trademarks of the particular copyright holder.
All rights reserved. Specifications are subject to change without notice.