PLANCK SECURITY

PLANCK SECURE EMAIL

The easy email encryption tool

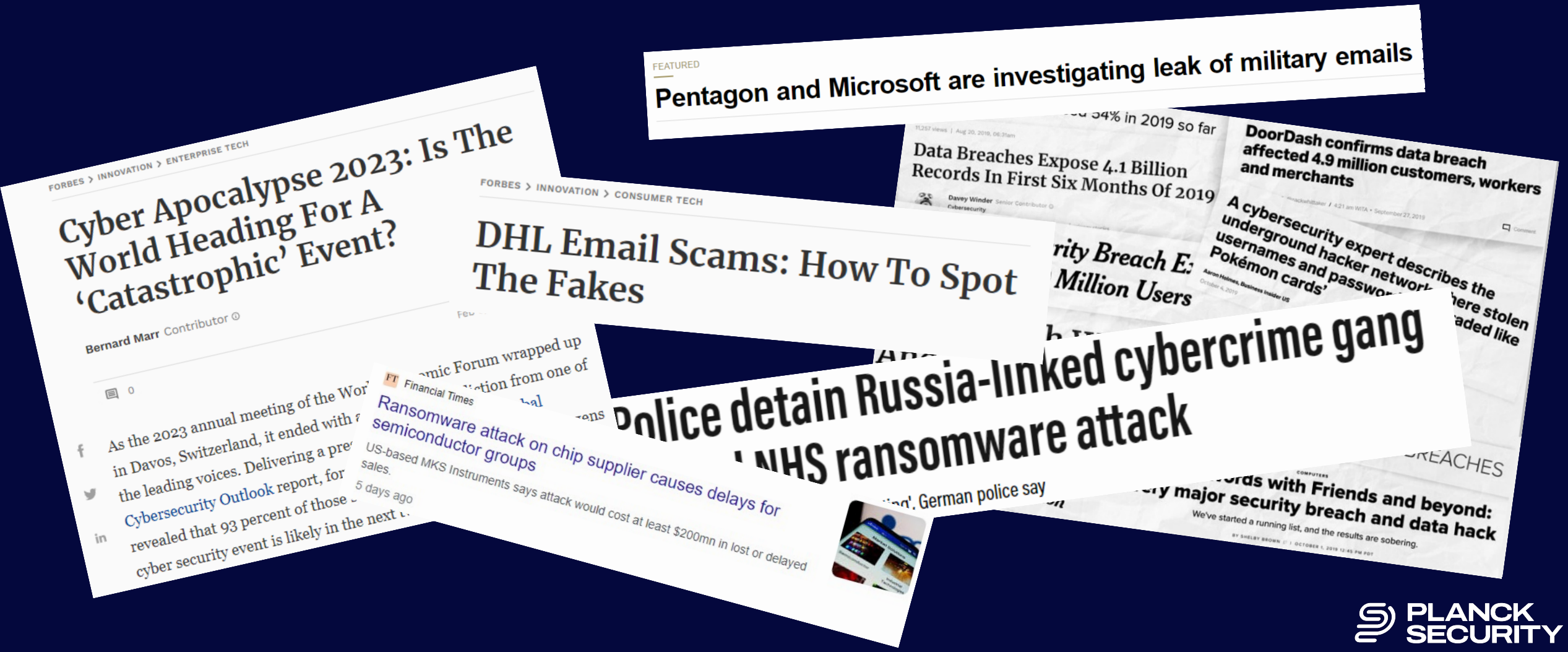
https://www.planck.security/

PLANCK SECURITY

#Imagine - sending a confidential email is as easy as talking to the person next to you.

PLANCK SECURITY

The Problem



https://www.planck.security/

PLANCK SECURITY

Cybersecurity Needs to Change

global cybersecurity spending exceeded $1 trillion cumulatively over the five-year period from 2017 to 2021

countless “improvements” (MFA, just saying) but: ever-high amount of security incidents

so - let’s go back to the the drawing table

PLANCK SECURITY

New Cyber Security Requirements

In order to adhere to **Zero Trust** principles, fundamental changes are required:

Trust nobody

Assume the enemy is inside

Encrypt all data in transit

Prevent any lateral movements by un-authorized parties

Monitor all traffic and activity

The only way to achieve these is to move away from central storage and move to a **peer-to-peer** trust and key management framework

This is what planck does

PLANCK SECURITY

Email is still attacking vector #1

91%

of targeted attacks start with email [1]

33%

Click-through rate [2]

14%

increase of unique phishing campaigns in Q1/21 [3]

212d

Days to detect to detect a data breach [4]

Phishing attacks lead to ransomware attacks or data breaches.

Confidential data in email stored on public cloud providers lead to loss in reputation, high legal fines, disruption of business.

PLANCK SECURITY

The Problem

EMAIL ENCRYPTION IS EITHER TOO COMPLICATED OR NOT TRUSTWORTHY

PLANCK SECURITY

Executive Summary

planck Security is the next generation of email encryption and trust verification

planck fully automates key, identity and trust management

planck acts as an Email Firewall on the endpoint

planck is fully compatible with all E-Mail Providers, incl. Microsoft365

planck eliminates all complexity in key and trust management through seamless integration with no visible change in user experience resulting in lower costs and higher levels of security

planck is a novel way to encrypt and verify trust of emails avoiding pitfalls and identity management issues with SMIME and PGP based protocols

PLANCK SECURITY

Planck Is the Answer

planck enables **every employee** to **encrypt and secure** emails without **any noticeable difference in user experience** and without **any pre requisite IT expertise**

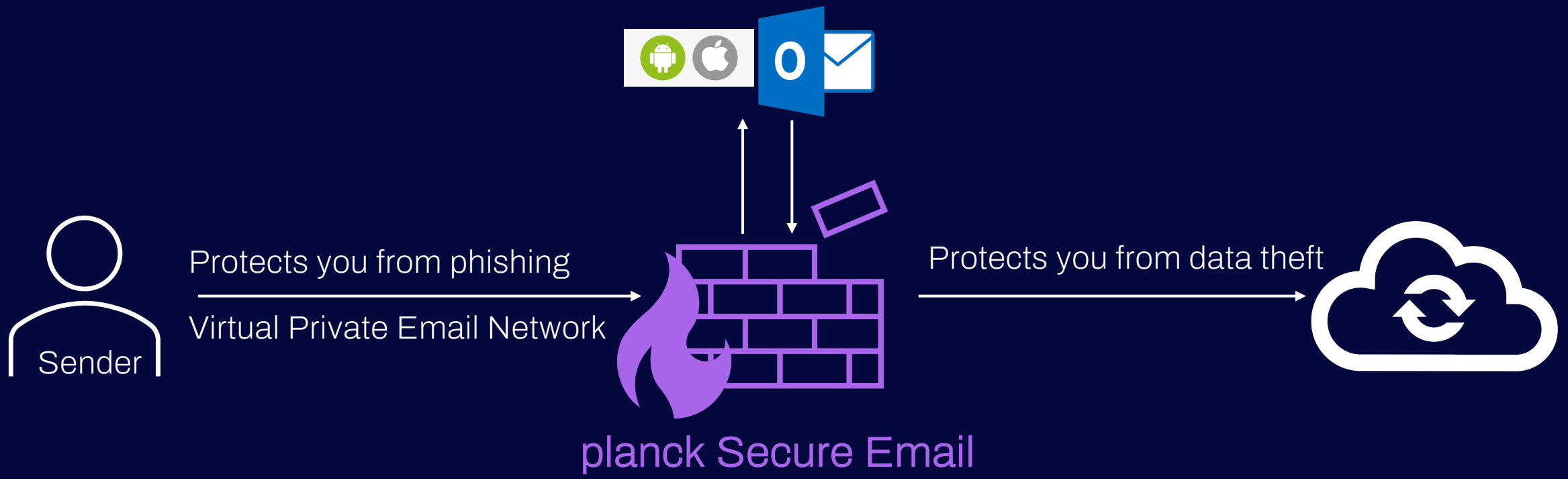
planck is **independent** from large tech IT providers adding **sovereignty** and **vendor risk diversification** into the key email communication channel

planck complies with **Zero Trust Architecture** to the **highest level** of adherence; Optimal (100% NIST SP 800-207)

planck is currently undergoing **BSI Common Criteria EAL2 Certification**

PLANCK SECURITY

Like a Firewall and VPN. But for Email.



PLANCK SECURITY

Advantages

User Friendly Interface

- No Interaction required
- Visual Security Status
- Guided User Experience

Automation

- Key Lifecycle Management; Generation/Prolong/Revoke
- Key discovery and Key renewal
- Private Key Handling
- Peer-to-peer Synch of Keys

Security Features

- Keys are generated on **each** device
- Trust is established **between** devices
- **No** reliance on central instances
- Encryption at rest **and** in transit
- End-to-end encrypted **even** for cloud based email
- **Full** Zero Trust Architecture

planck requires zero maintenance and is invisible to users

PLANCK SECURITY

It Is Decentralised

Decentralised peer-to-peer key & identity management

Unlike traditional encryption key management processes, planck is based on a cryptography architecture that does **not** rely on centralized key management nor storage thus **removing the single point of failure** element and making planck secure email **more secure.**

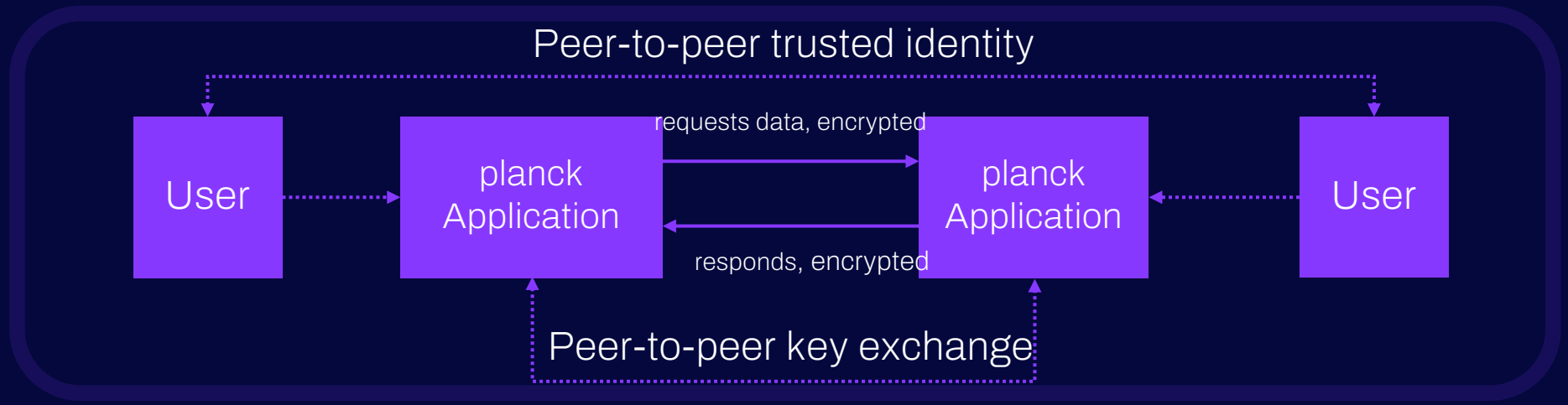
planck sits on every endpoint without a central element making **every endpoint individually protected**

Traditional encryption key solutions rely on CA's and their non-standardized black box processes. They are often compromised resulting in vulnerability or unavailability of service.

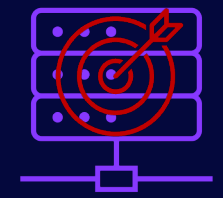
PLANCK SECURITY

Architecture

planck is a **new** approach to cyber security based on a unique **peer-to-peer** security architecture



No Central Instance



No Single Point of Failure

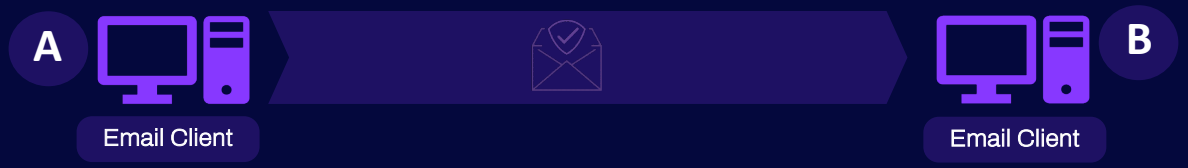
planck ensures encryption and protection is done on the endpoint itself ensuring that hackers need to not only obtain credentials (i.e. passwords) but also the actual device in order to gain access. Enabling this in an automated, seamless and user friendly manners is a material step forward in cyber security

PLANCK SECURITY

Next Generation Solution

Next Generation planck Secure Email Solution

A and B communicate seamlessly using planck Secure Email



Traditional Certificate Handling with Central Instances

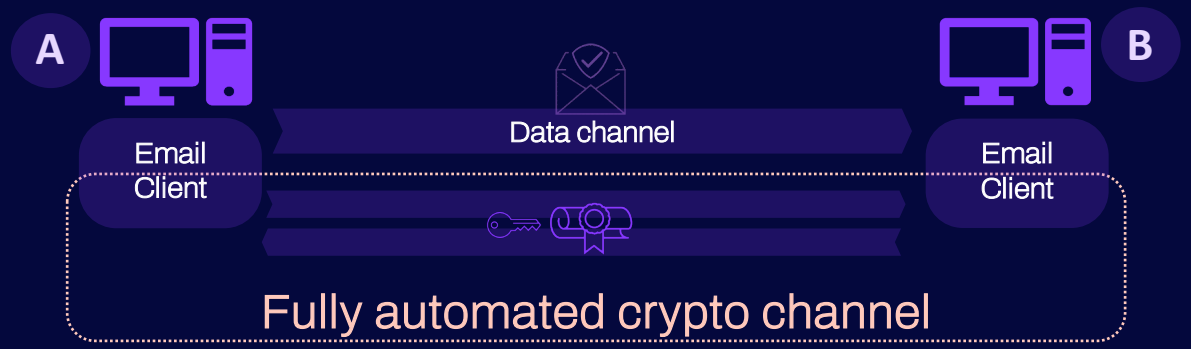
1: A registers its Identity with the RA
2: The RA transmits a new Certificate to the Central Certification Authority which in turn issues the certificate to A
3: The VA confirms the Identity of A by validating the certificate allowing A and B to communicate

https://www.planck.security/

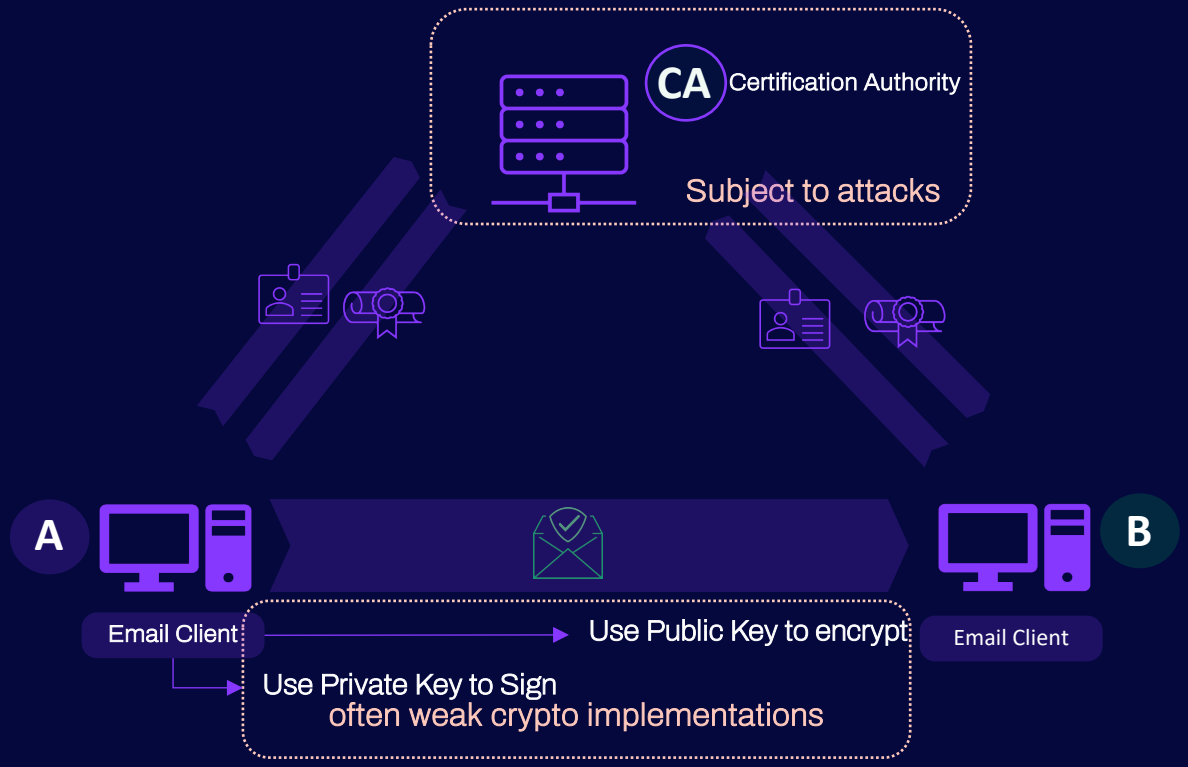
PLANCK SECURITY

Compared to S/MIME

There are no CA‘s involved
Users do not have to configure anything manually



S/MIME depends on CA’s and all their short comings[1]

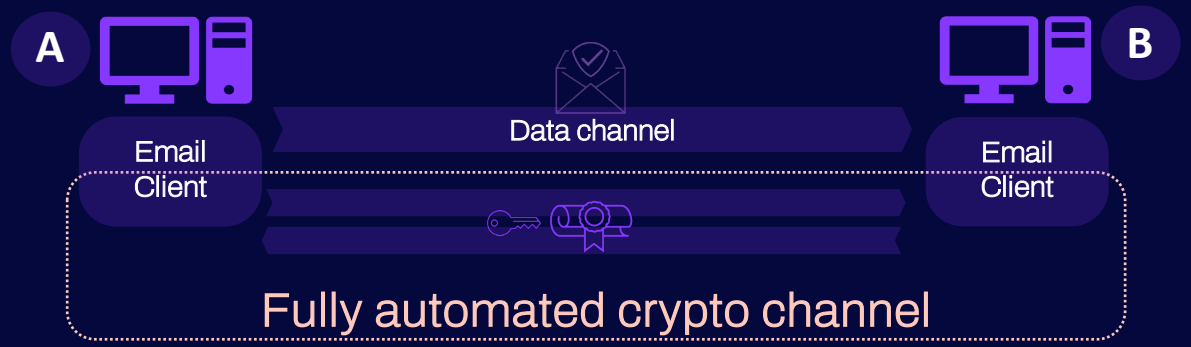


[1] for instance: https://nakedsecurity.sophos.com/2013/01/04/turkish-certificate-authority-screwup-leads-to-attempted-google-impersonation/

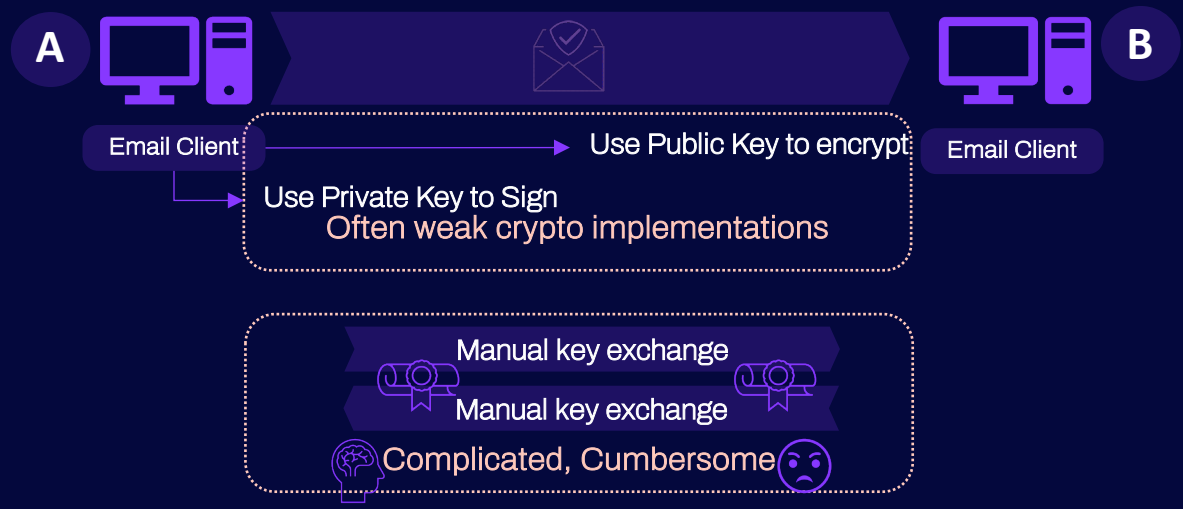
PLANCK SECURITY

Compared to PGP

There are no CA‘s involved
Users do not have to configure anything manually



PGP can be implemented **without CA’s**, but key management is **cumbersome**. Key Servers can help, but are subject to **attacks and operational issues.**



PLANCK SECURITY

Email Attack Patterns

Every email sent using planck secure email is **encrypted** with the receivers public key and sender **authenticated across enterprise boundaries** using the planck peer-to-peer encryption engine. This protects against know the most important vulnerabilities:

Eavesdropping (man-in-the-middle)

Identity spoofing (mailsploit)

Central system attack

Efail

Data theft

PLANCK SECURITY

Attack Protection

Eavesdropping: Attackers who intercept messages cannot read planck encrypted content. In contrary to PGP or S/MIME, planck also encrypts the meta-data such as headers and the subject lines. planck also implements advanced security measures, like Perfect Forward Secrecy.

Data Theft: Attackers that monitor the network or gain access to a user's mailbox cannot read the messages and don't gain access to data that is sent via email content, including the headers. This means, the content of an email is securely stored even in Cloud-based Email Providers

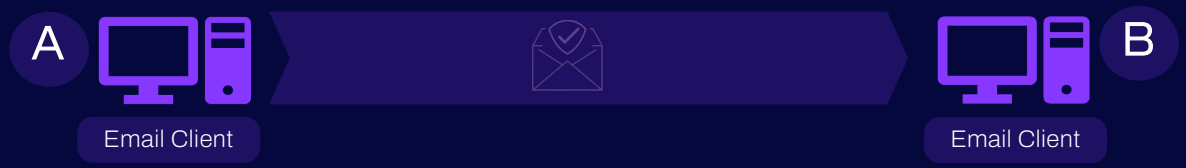
Mailsploit: Attackers spoof email identities to impersonate trusted communication partners. Mailsploit takes advantage of the standard RFC-1342. It uses it to encode non-ASCII characters and manipulate the "From" e-mail header. Hence, a carefully crafted string can be used in the "From" e-mail header, leading to identity spoofing and in some cases to code injection. What makes the attack possible, is the fact that e-mail clients and web interfaces do not properly sanitize the string in the "From" header after they decode it. This is a severe omission: in web interfaces and application APIs, non-validated (user) entries are the main cause of code injection. planck prevents this type of exploit

EFAIL: is an exploit based on two attack vectors: 1) model mismatch, "HTML" body is mapped to multiple HTML leaves in MIME tree 2) unauthenticated crypto packages. It allows hackers to exfiltrate content, even if the mail has been encrypted. Missing signature checks in PGP or S/MIME implementations make it relatively easy to execute an attack, given an intruder has access to the transport channel. Attackers who use the EFAIL exploit to gain access to content of encrypted emails are effectively prevented as planck prevents the use of message fragments to compose HTML messages, which is at the core of this exploit

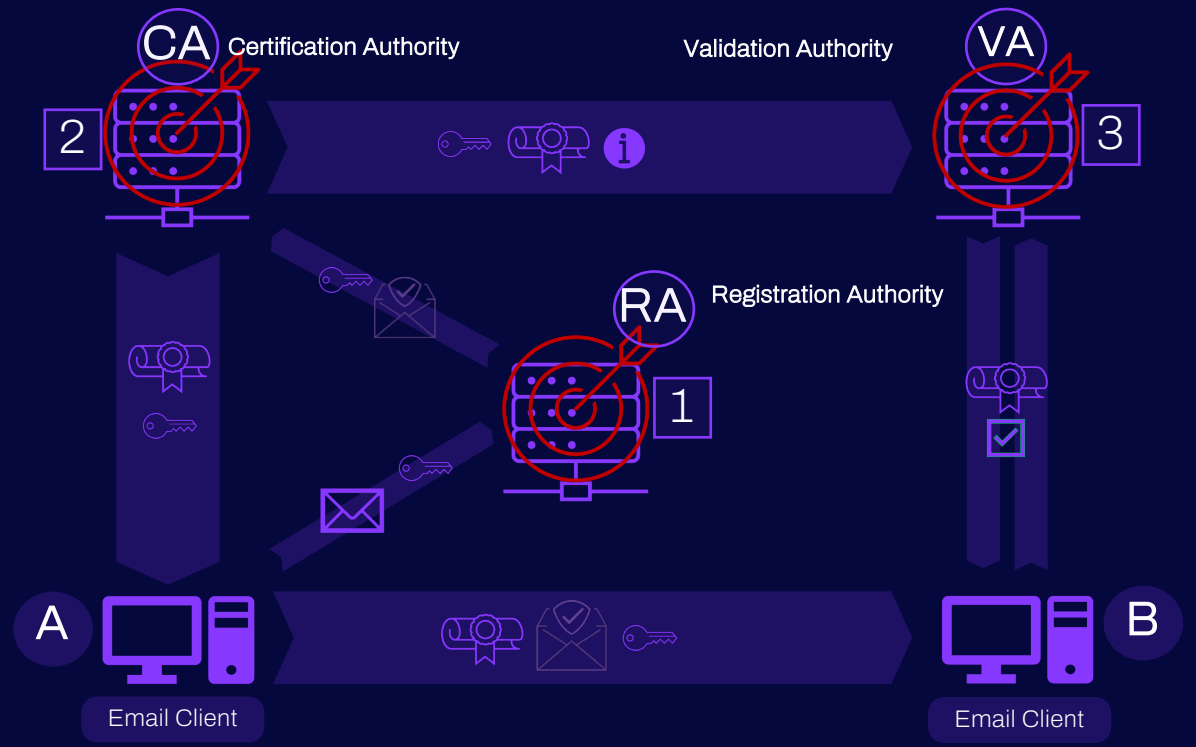
PLANCK SECURITY

Central System Attacks

planck is not vulnerable to central system attacks
There's simply no central system involved that could become unavailable or undermined



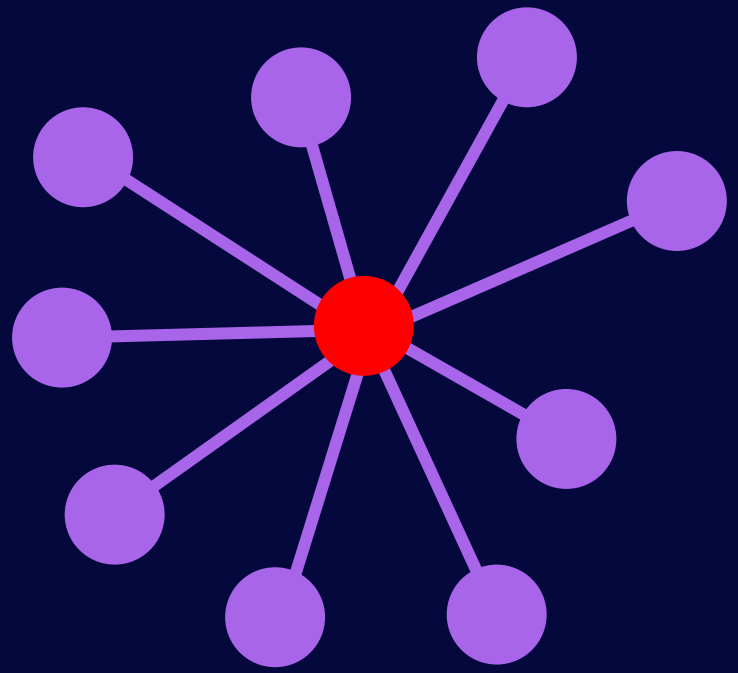
Traditional Certificate Handling with Central Systems



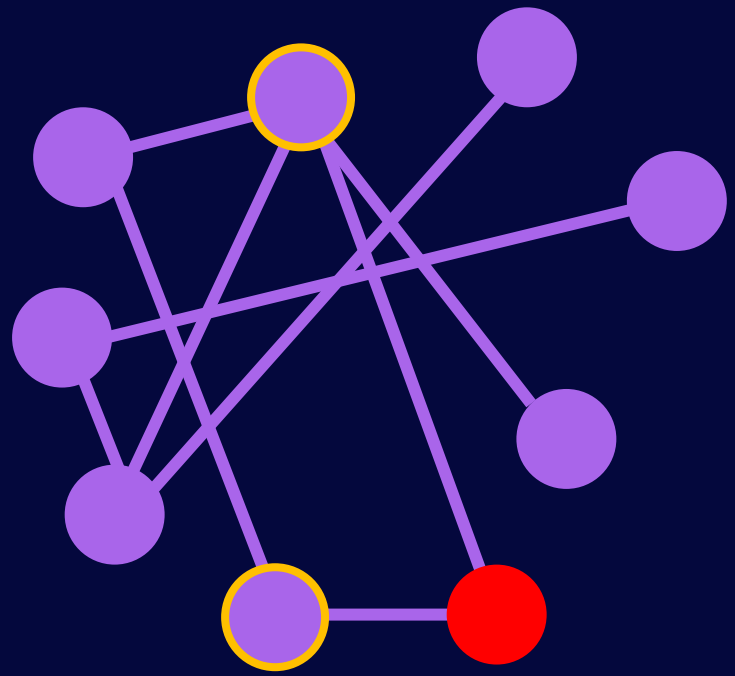
PLANCK SECURITY

Central vs. Distributed Trust

Winner takes it all



Adversary can do only local damage



PLANCK SECURITY

Eavesdropping

Like PGP or S/MIME, attackers who intercept messages cannot read planck encrypted content. However, planck also encrypts meta data of an email, as well as implement advanced measures like Perfect Forward Secrecy.

How planck does it?

planck encrypts and decrypts emails end-to-end in a fully decentralized way meaning the encryption happens on the sending system, the decryption on the receiving system, and at no point is the unencrypted information available to any third party. Keys are generated in each system by itself; trust is established between two systems (first step Trust-On-First-use (TOFU), second step verification via check of trustwords); **at no point there is any involvement of central instances necessary, like Certificate Authorities, Key Servers etc.**

Why planck does it better?

planck also encrypts the meta-data (header and the subject lines). Keys of communication partners and their trust statuses are managed and checked on a per-message basis. planck‘s trust model is 100% peer-to-peer. This prevents eavesdropping on the path between sender and receiver since the traffic is sent encrypted on-the-wire for its entire time in transit.

PLANCK SECURITY

Identity Spoofing

Phishing/spear-phishing/social engineering attacks delivering malware/ransomware and data theft

How planck does it?
planck verifies the authenticity of each distributed key and ensures emails are sender authenticated which means each email is signed and the identity is connected.

Why planck does it better?
planck ensures each user identity is connected to one e-mail address and a single key pair associated to a specific device. This means compromised passwords do not lead to security breaches.

The planck Security Status visually indicates the current security level of an email making it very easy to spot an unencrypted or manipulated email.

PLANCK SECURITY

Planck vs Alternatives

	planck email	Gnu Privacy Guard	Cryptovision GreenShield	S/MIME	Microsoft*
Identity spoofing (mailsploit)				Certain implementations	
Data Theft					
Efail				Certain implementations	
Central system attack	Key				
Eavesdropping (man-in-the-middle)		Certain implementations			

Key Legend:

Achieved | Not by default | Not covered

*Legacy OME / IRM in AD RMS / Purview Message Encryption

https://www.planck.security/

PLANCK SECURITY

Product Properties

planck product properties enable state of the art security without complicated user interaction and minimal admin-effort

There is no central element where secret keys are stored (also not with the CISO or Admin)

All emails are encrypted including headers and attachments fulfilling ZTA requirements

Private keys can also be brought to the devices de-centrally

A key reset can be initiated through software without input from users

Initial provisioning is possible using Microsoft Active Directory and GPO and Microsoft Intune

PLANCK SECURITY

Security Features

	planck email	Gnu Privacy Guard	Cryptovision GreenShield	S/MIME	Microsoft*
The communication partners are mutually identified		Not Automatic			
The communication is kept confidential				Weak Implementation	
The communication is authenticated					
Multiple Trustlevels					
No central repository of public and secret keys		Often implemented with public key repositories		Often implemented with central repository	

Key Legend:

Achieved | Not by default | Not covered

*Legacy OME / IRM in AD RMS / Purview Message Encryption

https://www.planck.security/

PLANCK SECURITY

Security Features

	planck email	Gnu Privacy Guard	Cryptovision GreenShield	S/MIME	Microsoft*
End-to-end encryption					
Receive S/MIME email					
Receive OpenPGP email					
ZTA maturity level	KEY				
Send OpenPGP email					
Email message encryption					
Email subject encryption	KEY				
Email attachments encryption					
Email signature					

Key Legend:

Achieved | Not by default | Not covered

*Legacy OME / IRM in AD RMS / Purview Message Encryption

https://www.planck.security/

PLANCK SECURITY

Planck in Practice

planck can be installed in 2 minutes

1. Install (plug & play) **planck** email on your desktop and/or mobile device

2. Connect your email account

3. Start sending people (encrypted) email
- If counterpart has **planck** all email will be encrypted after the first email, where the public keys are exchanged
- If counterpart has no **planck**, email will be sent unencrypted
- Note: Add an additional level of security through the exchange of trust words between users in **planck**. All email will be labelled as either trusted, secure, insecure or not encrypted to easily distinguish security levels.

PLANCK SECURITY

Provisioning

Unlike traditional encryption key management tools, planck is **fully automated** and **runs seamlessly** in the background removing all complexity and ensuring **all employees** can **effortlessly** send and receive secure emails.

planck Secure E-mail is designed to bring the software to the endpoint as a client or plug-in and runs agnostically with any EPS, MDM, and IAM or SSO.

planck uses the authentication functionality of the device operating system as a basis for the automated sender authentication for each message.

As such, planck is directly compatible with any EPS, MDM, and IAM or SSO that also relies on the operating system's authentication for its own source of identity.

The software is **self provisioning** (no running admin) and plug-in based making it **seamless**

Lower operational risk for the user

Making planck operationally more robust

PLANCK SECURITY

Compatibility

planck compatibility with existing security architecture if required

If required the **planck proxy** inserts an in-band end-to-end relation between mail-clients. It doesn't matter which additional security features like VPN, TLS, Access Gateways, Segmenting etc. are used in the network. planck always provides security

Central virus scanners that are using filter out mails with unreadable content can be configured to forward encrypted email

planck secure email establishes an additional secured layer of identity without any dependency to other identity concepts

PLANCK SECURITY

User Features

	planck email	Gnu Privacy Guard	Cryptovision GreenShield	S/MIME	Microsoft*
Send/Receive email (1 step approach)					
Key management (without requiring user interaction)	KEY				
Group mailbox	KEY				
Access secure email from defined group of devices					
Mobile applications					
Integrate 3rd party SEG / DLP					
Easy public key exchange					

Key Legend:

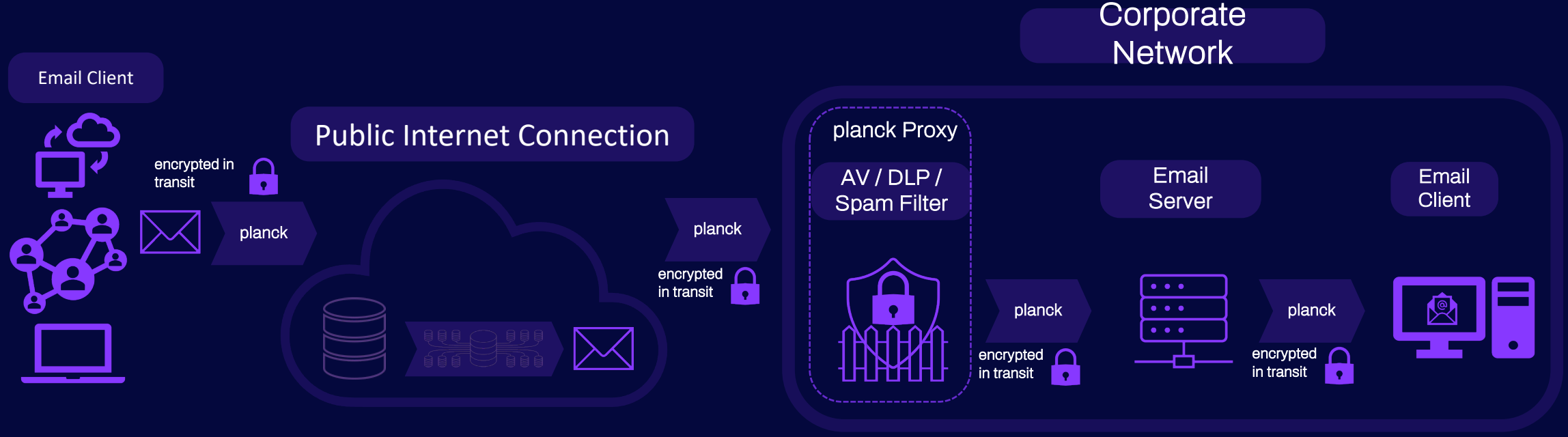
Achieved | Not by default | Not covered

*Legacy OME / IRM in AD RMS / Purview Message Encryption

https://www.planck.security/

PLANCK SECURITY

Communication Architecture



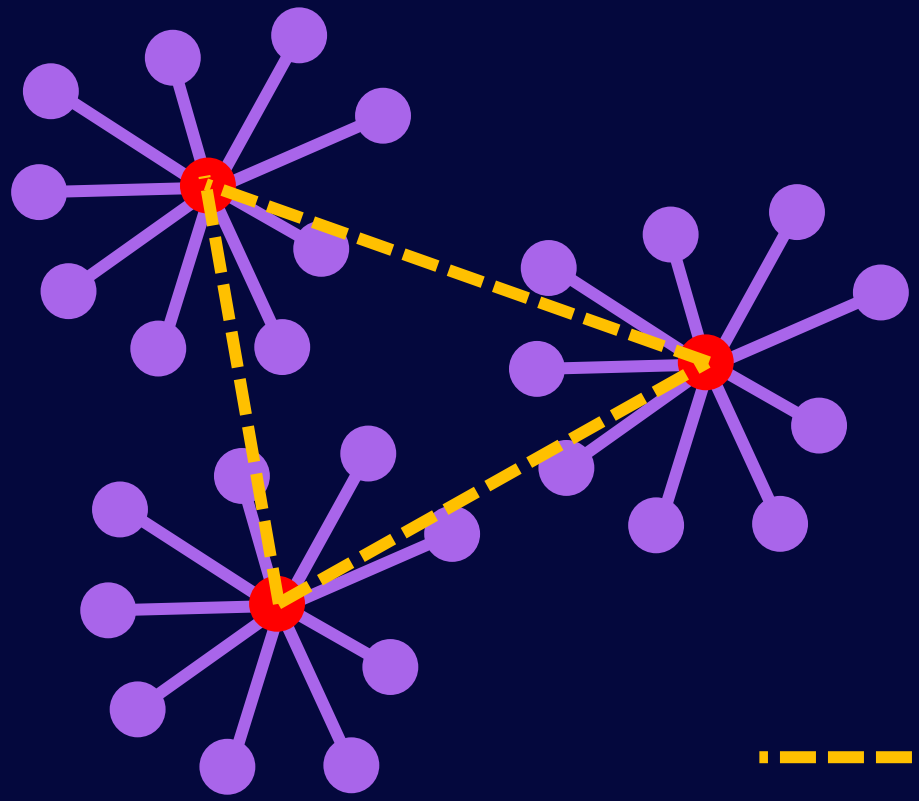
End-to-End Protection

https://www.planck.security/

PLANCK SECURITY

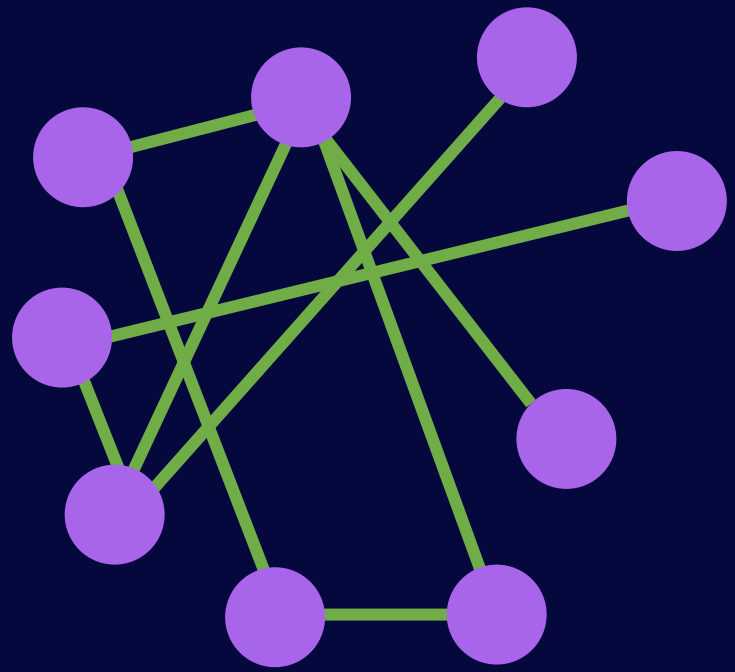
Cross-Enterprise Trust

Cross-enterprise trust is complex, expensive, does not scale very well



manual

No PKI-cross trust means - scales for thousands of partner companies



fully automated

PLANCK SECURITY

Software Architecture

planck has a modular stack

Catering to many applications

Applications

planck Outlook plug-in | planck for Android | planck for iOS

Interfaces

COM Server Adapter | JNI Adapter | Objective-C Adapter

Key Management

planck core

Crypto Engine

Crypto Stack (sequoia-pgp, botan, ...)

Concept

Implementation

https://www.planck.security/

PLANCK SECURITY

Engine Functionalities

The planck Engine is the core component of every planck enabled app

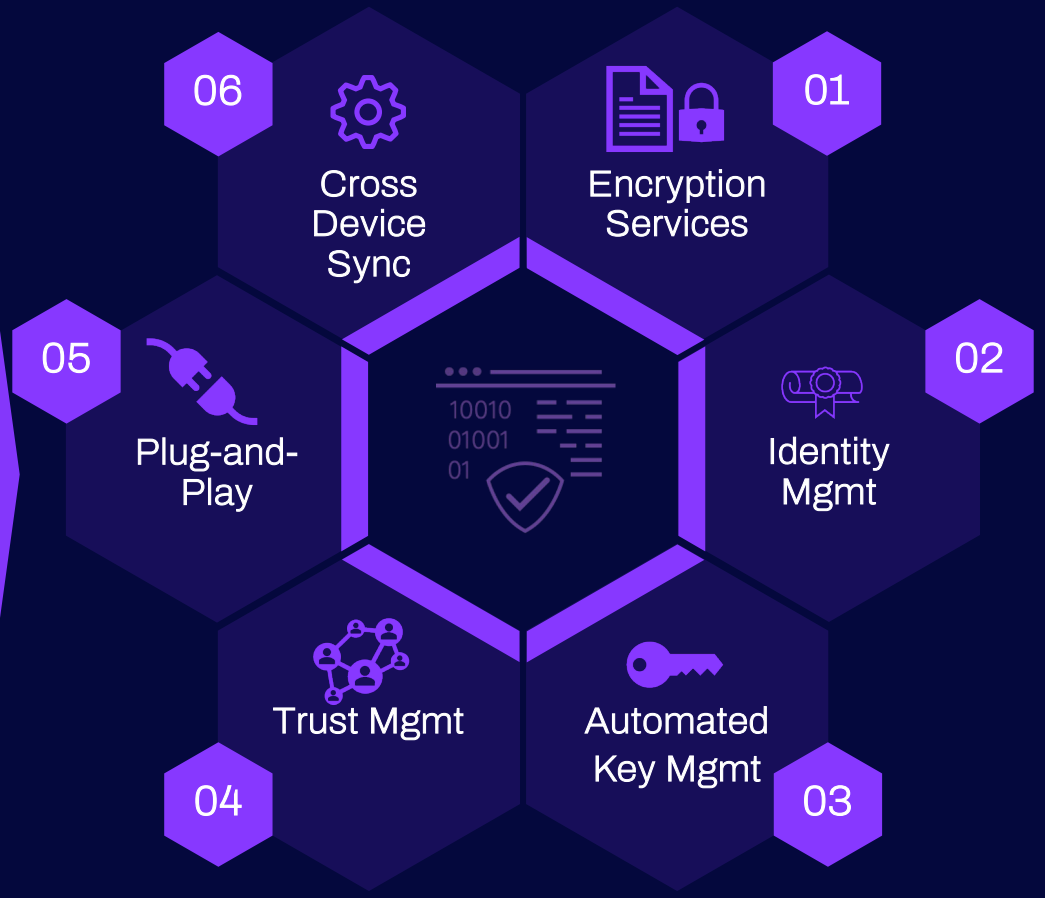
A library, which applies cryptography to messages, manages keys, handles trust, and drives message transports

The Engine allows for complex security functionality via much simpler planck protocols

The planck Engine does this by isolating much of the security-critical code in a single, internal component

The planck Engine is written in C17

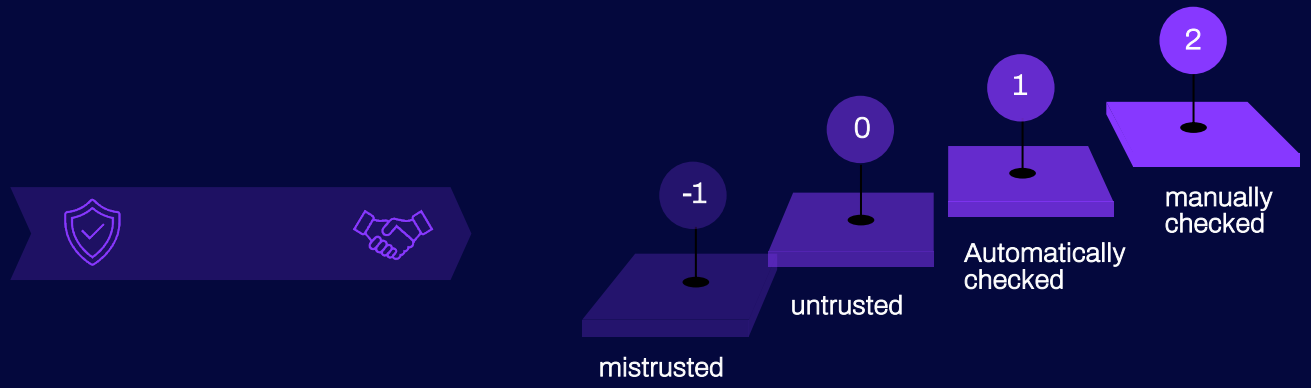
This planck Engine is highly portable and can run on diverse software and hardware



PLANCK SECURITY

Trust Levels

planck Trust consists of different trust levels:



Different implementations can be used in **planck** for implementing these trust levels:

- **TOFU** for **level 1** and;
- **Derived fingerprints** for **level 2**

In **planck** Secure Email, trust is defined between a User and Key

PLANCK SECURITY

Process – Proctecting the First Message

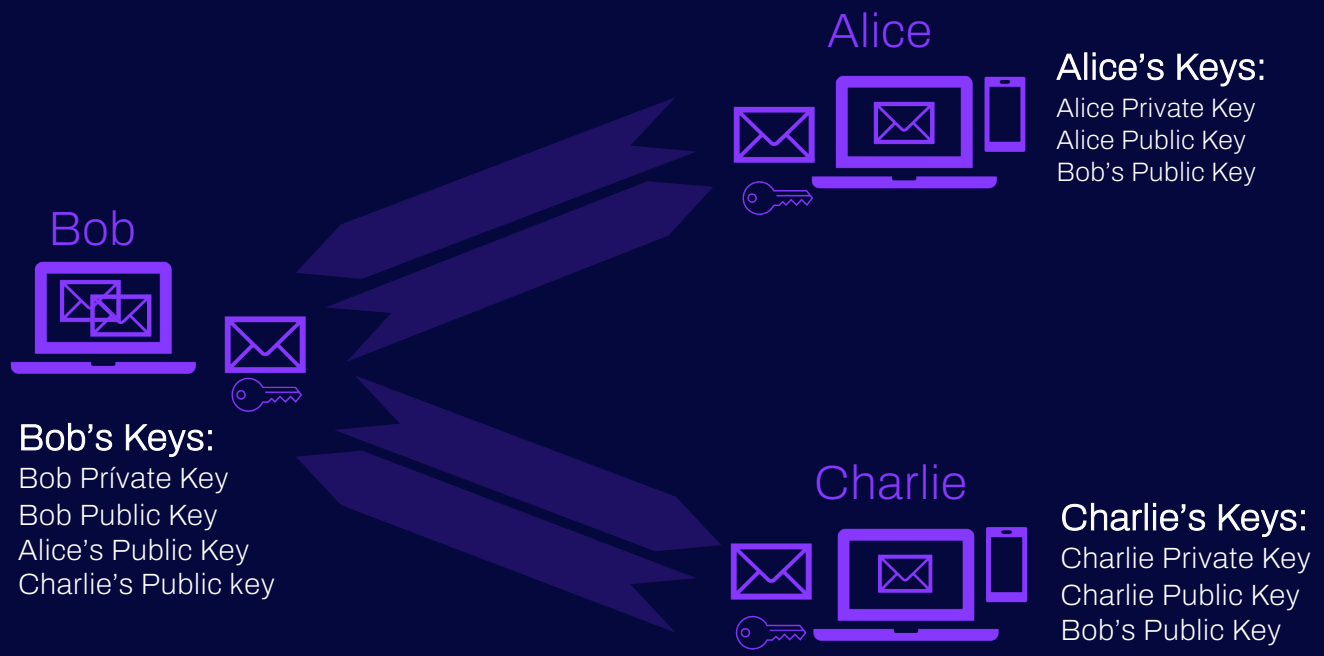
Trust On First Use (TOFU)
planck's Automatic Trust Model is based on TOFU.

A Secure Channel is established between the two users by certificate pinning.

The Communication Partners are mutually identified (Claim / Fulfilment):

Claim
in inner message / is signed: This is my key, the "Sender's Key".

Fullfilment
in outer message: Delivery of public key material for exactly this key, coming from the exact identity, which is "From:"

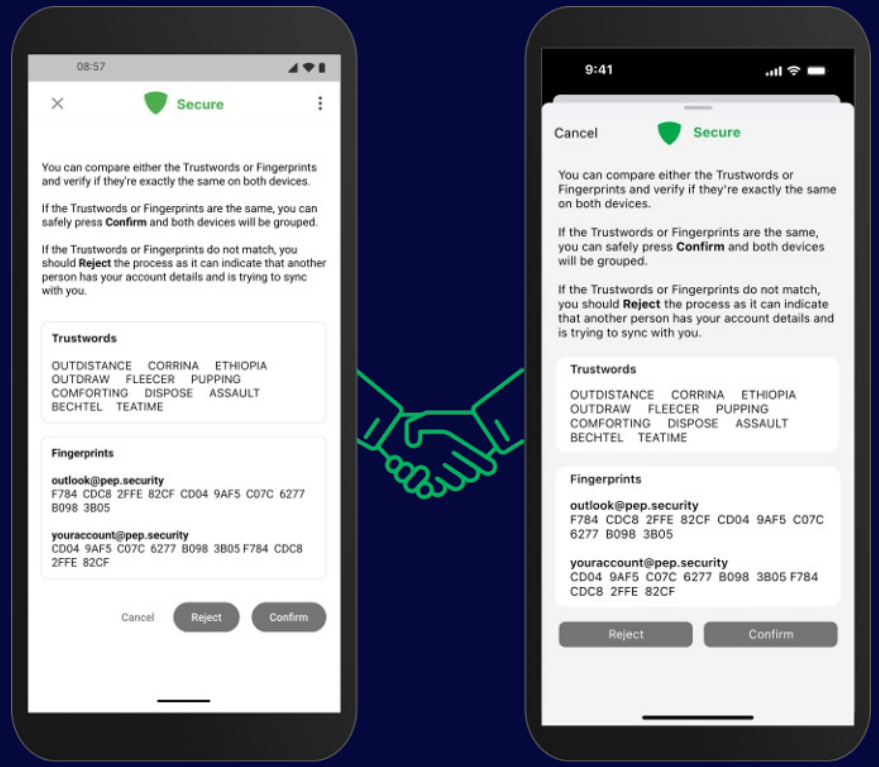


PLANCK SECURITY

Verified Trust

To further secure communication partners, planck allows for manual trust verification (Trust Level 2)

Derived fingerprints are calculated as dictionary lookup by RIPEMD-160 of the ordered two fingerprints of sender's and receiver's key.



PLANCK SECURITY

4 pillars of Zero Trust Email Security

Decentralised Identity

End-to-end encrypted

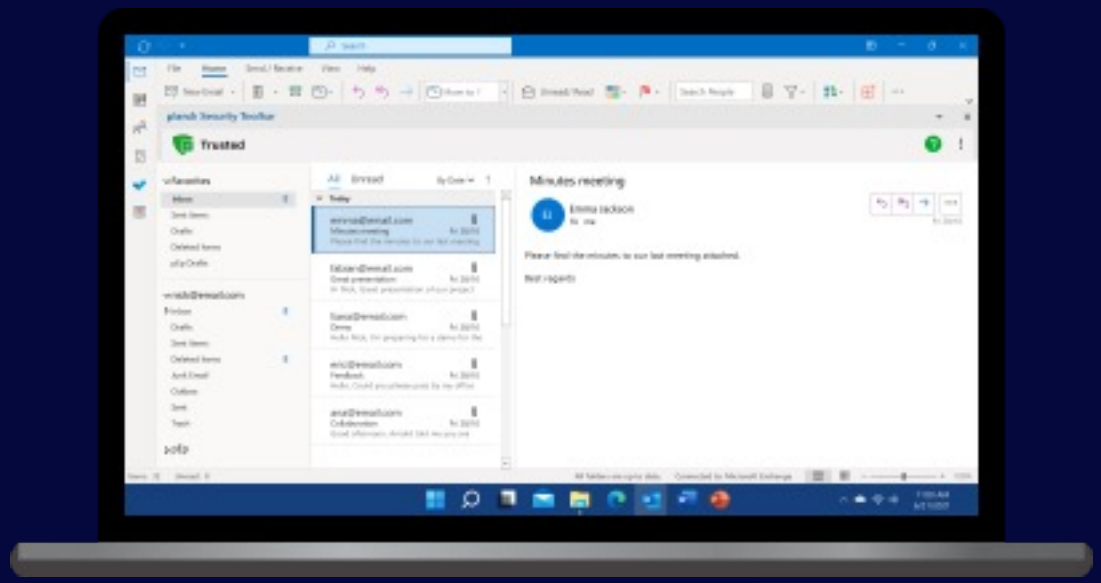
Seamlessly automated and non-intrusive

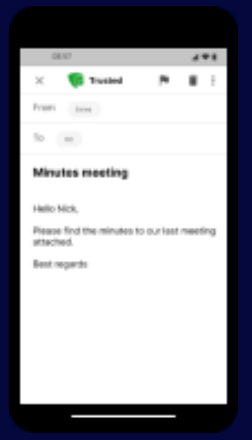
Utilises the highest performing crypto libraries

PLANCK SECURITY

Solution

- Seamless plug-in for **Microsoft Outlook**
- Standalone app for **Android mobile devices**
- Standalone app for **iOS mobile devices**
- *Roadmap/MVP Q4.23: Outlook Webmail*





PLANCK SECURITY

ZTA – Zero Trust Architecture

planck email is ZTA compliant by default

Perimeter-based cyber security has served its time. This is why the NIST (*National Institute of Standards and Technology: NIST SP 800-207) is calling for a paradigm shift: Zero Trust Architecture which uses zero trust principles to plan industrial and enterprise infrastructure and workflows.

Thanks to its ground-breaking software architecture and design developed on the premises of ZTA, planck is leading the way into the next generation of cybersecurity.

An official website of the United States government Here's how you know

NIST Search NIST Menu

PUBLICATIONS

Zero Trust Architecture

Published: August 10, 2020

Author(s)
Scott W. Rose, **Oliver Borchert**, Stuart Mitchell, Sean Connelly

Abstract
Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network- based perimeters to focus on users, assets, and resources. A zero trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established. Zero trust is a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud- based assets that are not located within an enterprise-owned network boundary. Zero trust focus on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource. This document contains an abstract definition of zero trust architecture (ZTA) and gives general deployment models and use cases where zero trust could improve an enterprise's overall information technology security posture.

Citation: Special Publication (NIST SP) - 800-207

Report Number: 800-207

NIST Pub Series: Special Publication (NIST SP)

Pub Type: NIST Pubs

PLANCK SECURITY

Still curious about email security?

Download the free trial version today. Email Encryption is just 2 minutes away!

www.planck.security # ip@planck.security

PLANCK SECURITY