iDENtear

Apply Mobile

iDENtear Overview

Who Are Apply Mobile?

- Apply Mobile are a technology company that provides authentication and access products and solutions
- Apply Mobile identified a significant gap in the market for an authentication and access device with good user experience, easy to use but yet very secure and centrally manageable
- Apply Mobile have been working on iDENtear which has been developed in our R&D facility in Helsinki, Finland

Current View on Authentication and Mobility

"In the absence of widely available and proven mobile-apt (or mobile-friendly) authentication methods, pragmatism is driving enterprises to implement methods that may not be classically "strong", but rather are technically feasible, are lower cost and provide better User Experience.“

Gartner Magic Quadrant for Authentication

December 2013

What is iDENtear?

- iDENtear is a Bluetooth contact-less Authentication and Access device
- iDENtear is computing device agnostic and can be used with Mobile Phones, Tablets, Laptops and Desktop computers are Bluetooth enabled
- iDENtear is an intelligent device within security hardware that can store credentials
- iDENtear can provide One-Time Passwords (OTP), SmartCard Access and integrate with web technologies such as Oath, SAML and OpenID

Traditional Hardware Device

Apply Mobile

Strengths

- Secure closed hardware
- Tamper Evident and Tamper Resistant
- Segregated from potentially compromised systems
- One device per user to many computing devices

Weaknesses

- Poor user experience and cumbersome on mobile platforms
- Cannot integrate with local Applications
- May require additional hardware readers
- Secrets burned into device within the factory
- Questionable manufacturing locations
- Offers little to protect against phishing or social engineering

Software Token

Strengths

- Easy to deploy
- Integrates with Applications
- Good user experience
- Easy to use

Weaknesses

- Shares computing resources with computing device
- Administrative effort - Each computing device needs to be enrolled
- Affected by Software vulnerabilities or malicious code within shared ecosystem
- 2nd factor on the same device as the 1st factor – and online
- Offers little to protect against phishing or social engineering
- May not meet regulatory mandates due to software offering or key management

How iDENtear Is Different?

Secure Hardware for Generation and storage of Secrets built to FIPS 140-2 Level 3

Can be used Online or Offline with Software SDK for online services or offline access

Secure Bluetooth for Application Integration, User Experience and Ease of Use

Ability to ensure no collisions of one-time passwords

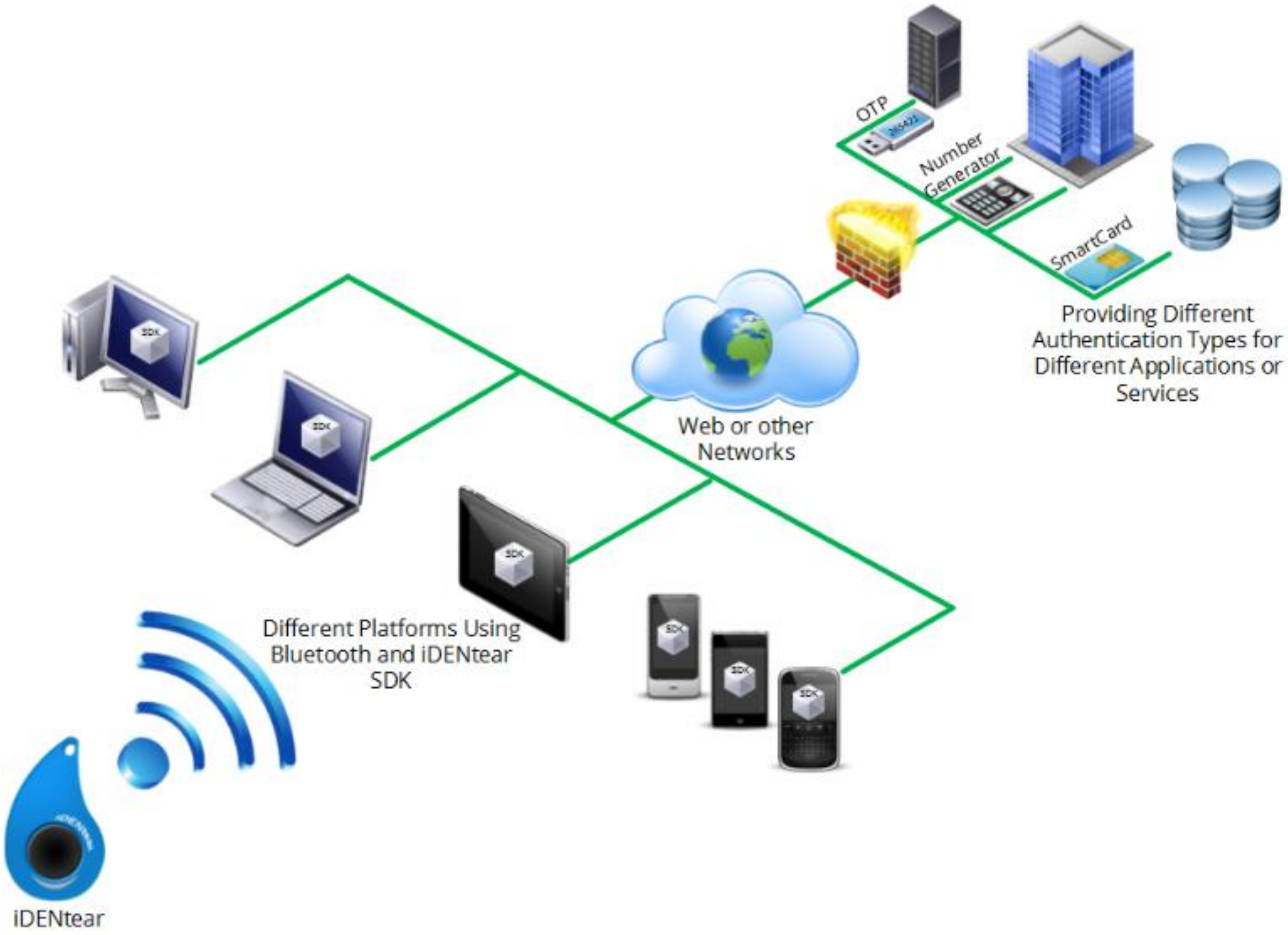
Proprietary Internal Hardware Random Number Generator

Ability to be Personalised with new credentials over the air

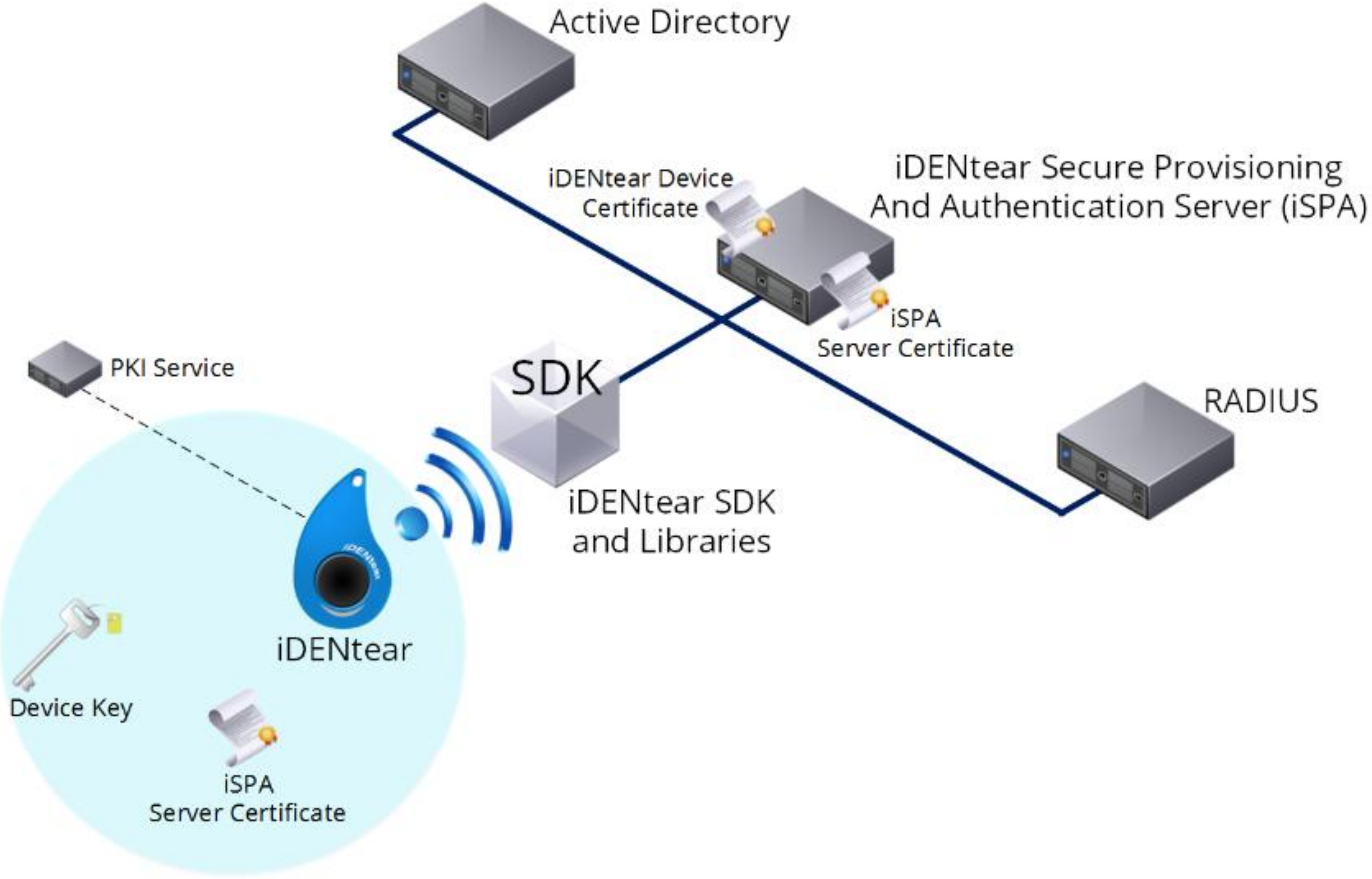
Industry Accepted Cryptographic Ciphers aligned to FIPS standards

Integrate into existing authentication technologies such as RADIUS and Active Directory

How does iDENtear Work?


OTP
Number Generator
SmartCard
SDK
Providing Different Authentication Types for Different Applications or Services
Web or other Networks
Different Platforms Using Bluetooth and iDENtear SDK
iDENtear

iDENtear Architecture


Active Directory
iDENtear Device Certificate
iDENtear Secure Provisioning And Authentication Server (iSPA)
iSPA Server Certificate
PKI Service
SDK
RADIUS
iDENtear SDK and Libraries
iDENtear
Device Key
iSPA Server Certificate

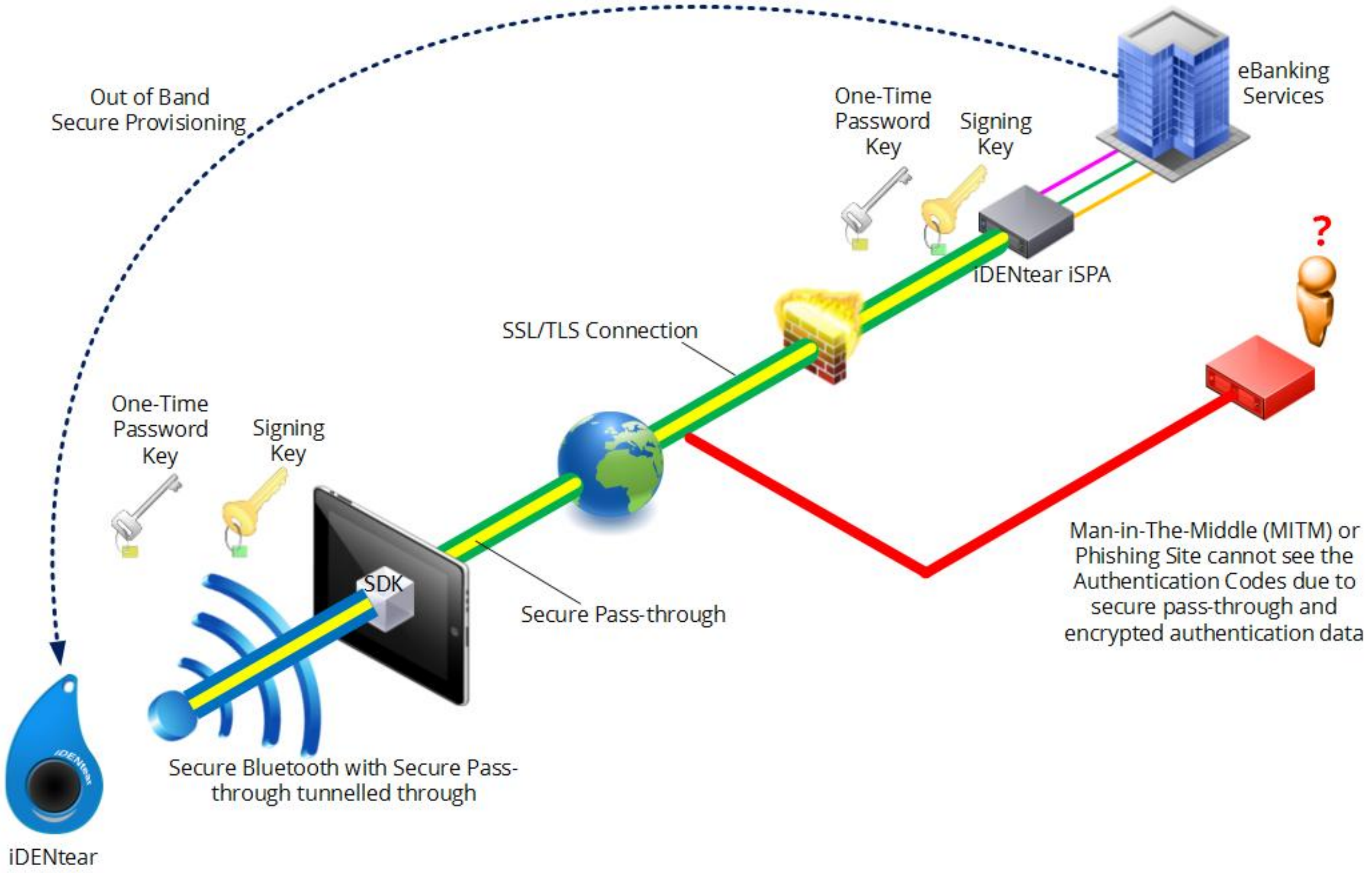
Benefits of iDENtear

- Strong Hardware based security
- Contactless Secure Bluetooth to multiple computing platforms
- Secure Pass-through Technology to prevent Man-in-The-Middle and Phishing Attacks
- Easy to provision and deploy to users – Deploy just once
- Great User Experience - User is fully engaged with the Service and not the Security
- One device per user to use on many computing devices
- Simple and easy to use – User simply clicks the button
- No other hardware readers required
- Tamper Evident, Tamper Resistant, dust and water proof
- Centrally Manageable and Ability to personalise over the air
- Meets regulatory Mandates due to Key Management and Hardware based Security

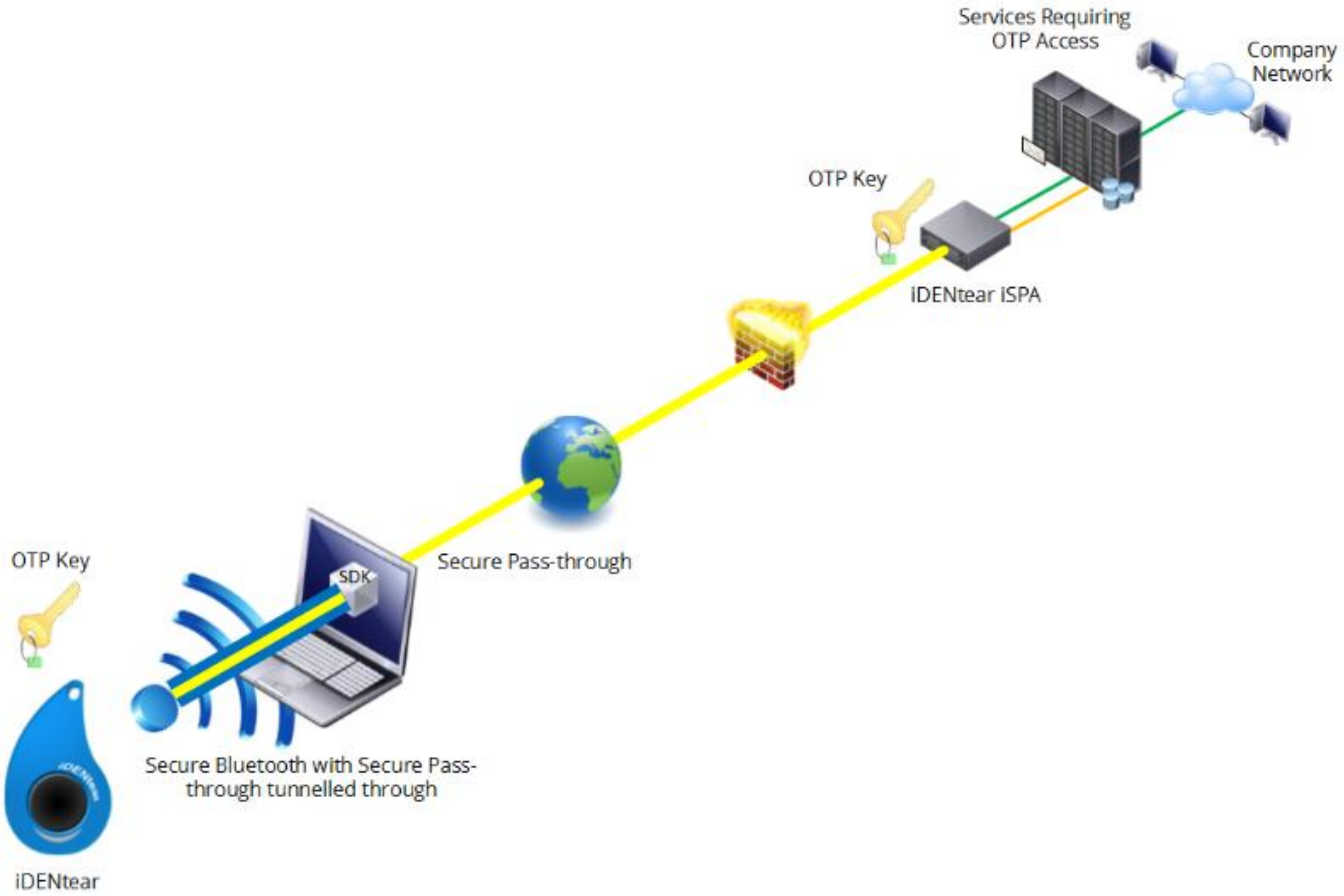
iDENtear's Ability to Thwart Common Threats

- Secrets are always generated on the device using hardware and not burned into device during manufacturing
- Secure Bluetooth used to connect to the device
- Secure Pass-through technology prevents Man-in-The-Middle and successful phishing attacks
- Can send authentication data with Digital Signature
- Ability to prevent OTP collisions – no concatenation for 6 digits needed
- Credentials in secure Hardware with no device presence on the Internet

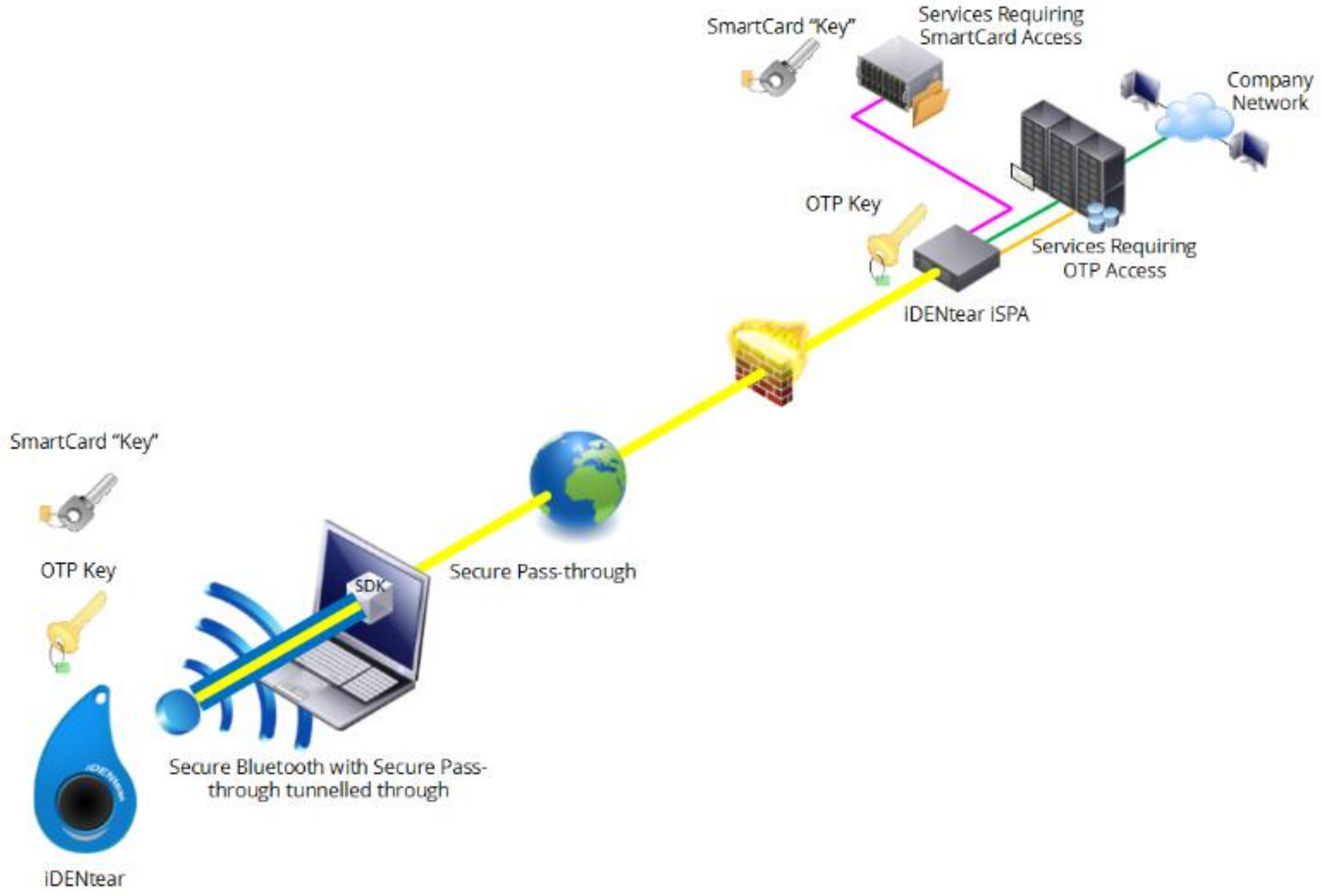
Use Case 1 – Banking Access



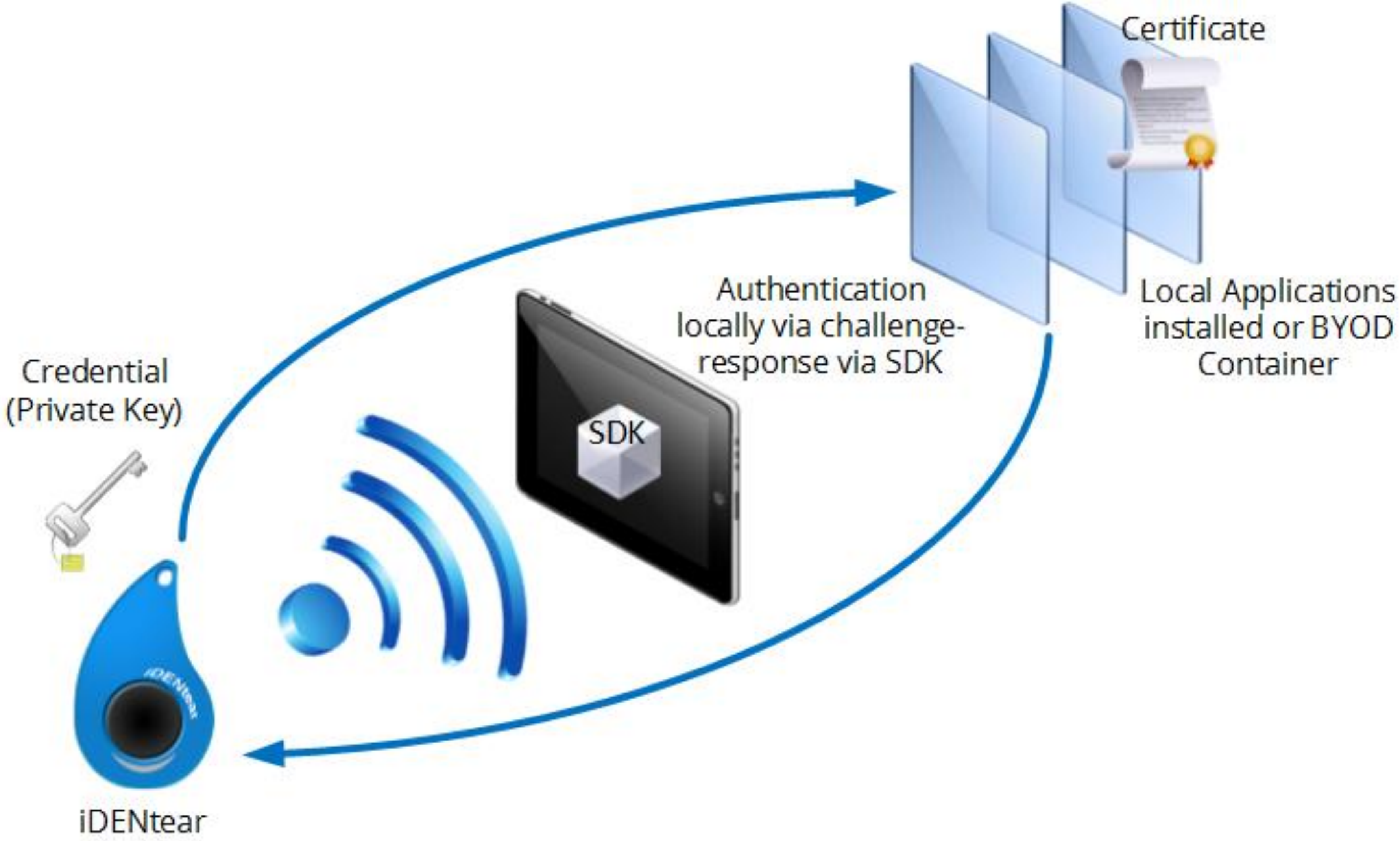
Use Case 2 – Remote Access



Use Case 3 – Remote Access and Data Access


SmartCard "Key"
Services Requiring SmartCard Access
Company Network
OTP Key
Services Requiring OTP Access
iDENtear iSPA
SmartCard "Key"
OTP Key
SDK
Secure Pass-through
Secure Bluetooth with Secure Pass-through tunnelled through
iDENtear

Use Case 4 – Offline Security


Certificate
Authentication locally via challenge-response via SDK
Local Applications installed or BYOD Container
Credential (Private Key)
SDK
iDENtear
iDENtear

iDENtear 2014 Roadmap

Apply Mobile

- Contextual Authentication based on assurance levels through biometric fingerprint reader to ensure non-repudiation and validation of identity.
- FIPS 140-2 Accreditation
- Physical building access
- Different form factors such as credit card shape and badge pass shape
- Custom corporate branding and shape

Device and Software Licensing

- Simplification of the Commercial Model
- One-off Cost of Hardware Device per user
- Service and Maintenance Cost per device per annum

Summary

- A convenient authentication device that uses Bluetooth to connect to a number of computing platforms
- Integration with applications via the iDENtear SDK
- Simple usage for the end user
- Secure Hardware for credential storage and management
- Secrets generated on the hardware device
- Digitally sign transactions
- Simple commercial model