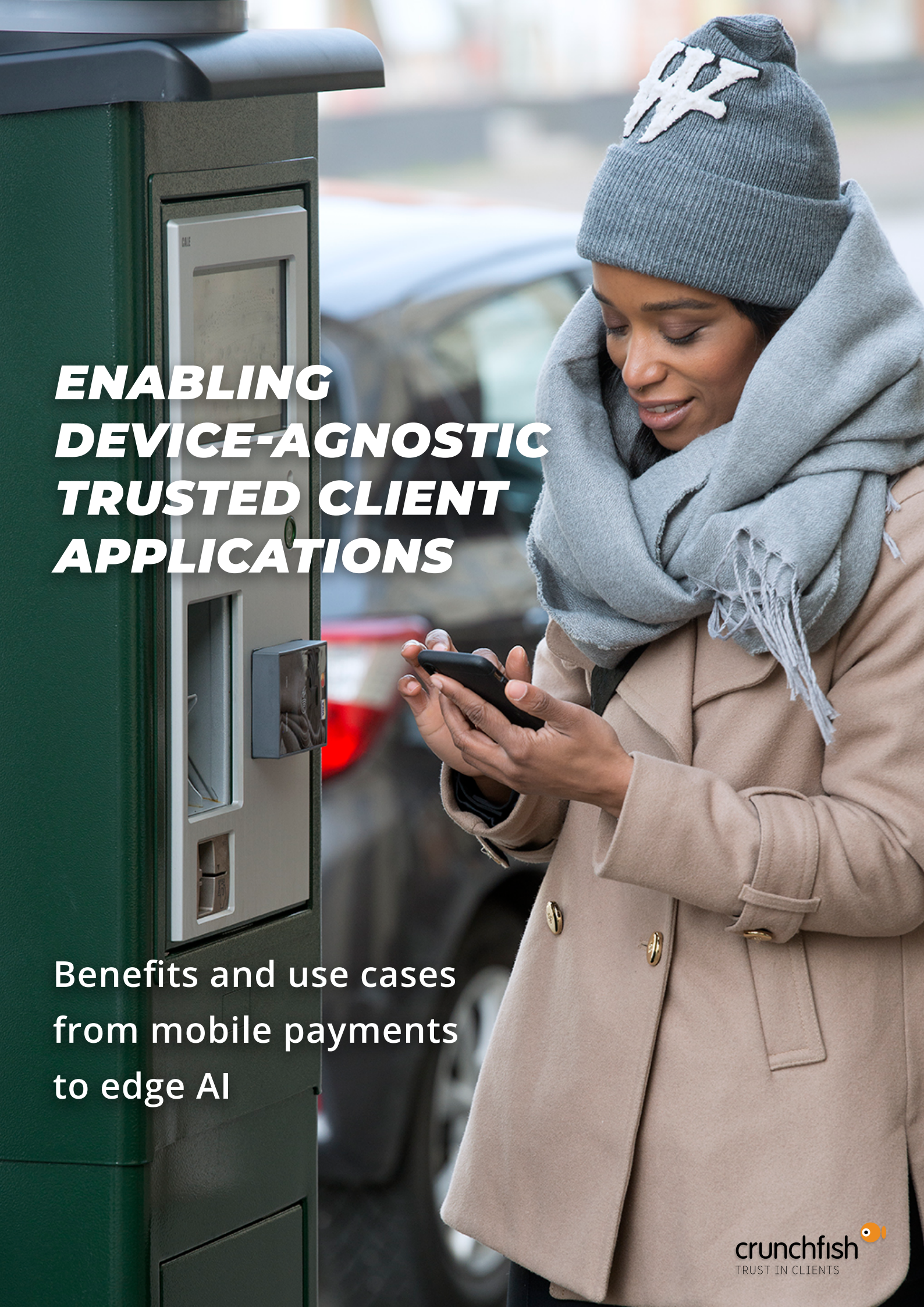

ENABLING DEVICE-AGNOSTIC TRUSTED CLIENT APPLICATIONS

Benefits and use cases from mobile payments to edge AI

crunchfish
TRUST IN CLIENTS

2024-06-05

Enabling Device-Agnostic Trusted Client Applications

Benefits and Use Cases from Mobile Payments to Edge AI

Whitepaper by Joachim Samuelsson, CEO, Crunchfish

This whitepaper delves into the critical role of device-agnostic trusted client applications across diverse verticals such as mobile payments and edge AI. Security, privacy, and resilience can be improved by providing a robust framework for processing data offline. It explores novel offline use cases and the benefits of leveraging such trusted client applications in handling sensitive data without constant connectivity to centralized servers.

Introduction

Crunchfish is a pioneer within offline payments. The challenge that Crunchfish has solved is how to implement trusted client applications that may be used to enable offline payment with mobiles, regardless of which device the user has. Crunchfish has created the only offline payment solution in the world that is both secure and device-agnostic at the same time[1]. The Crunchfish Digital Cash solution has been pilot tested in India by leading banks and in was approved in December 2023 by the Reserve Bank of India for rollout by regulated entities[2].

Crunchfish's technology can also be applied to mobile card payments by enabling device-agnostic trust in clients for tokenized card payments by a new form of card emulation App-integrated Card Emulation (ACE)[3]. ACE works like Host-based Card Emulation (HCE) but with the advantage that superior security is already built into the ACE software development kit. While the offline payment market is still in its infancy, there are 5 billion digital wallets with tokenized card payments. Crunchfish will take a position and become a pioneer in mobile card payments as well.

Offline and mobile card payments are not the only two use cases that benefit from Crunchfish's ground-breaking mobile application technology. In fact, mobile client / server applications in multiple market segments stand to gain, especially when assets are handled offline in the client. In addition to enabling novel offline use cases, a trusted client application improves the security in the system.

This whitepaper makes the case for trusting the mobile clients, even in offline mode. The whitepaper starts by describing the most important features that must be in place for trusting the application client and outlines key offline benefits and how they apply to market industries. The case is then made for device-agnostic trusted clients to have a solution that is possible to deploy in practice. This is followed by use cases in offline payments and explaining the key technical features that must be in place. The whitepaper then discusses various use cases related to edge computing in AI using device-agnostic trusted mobile clients.

---

[1] https://www.crunchfish.com/wp-content/uploads/2024/02/Crunchfish-whitepaper-Offline-payment-for-smartphones-20240201.pdf

[2] https://www.crunchfish.com/reserve-bank-of-india-approves-crunchfish-digital-cash-for-offline-retail-payments/

[3] https://www.crunchfish.com/wp-content/uploads/2024/04/Crunchfish-Whitepaper-ACE-THE-FUTURE-OF-MOBILE-CARD-PAYMENTS-20240415.pdf

Trust in clients

Trust in clients is based on the ability to securely handle data in offline mode: 1) during execution, 2) when data is stored, and 3) while in transit. The execution is especially vulnerable because data must be processed decrypted. This requires a Secure Element (SE) on the mobile device. To avoid limiting the user base to certain mobile devices, the SE must not be hardware dependent, but implemented in software as an app-integrated virtual SE[4]. Data at rest is stored on the mobile phone in encrypted files. For data integrity, it is necessary to be able to detect if these files have been tampered with. The security protocol of the application makes the communication secure end-to-end, avoiding man-in-the-middle attacks, while data is in transit.

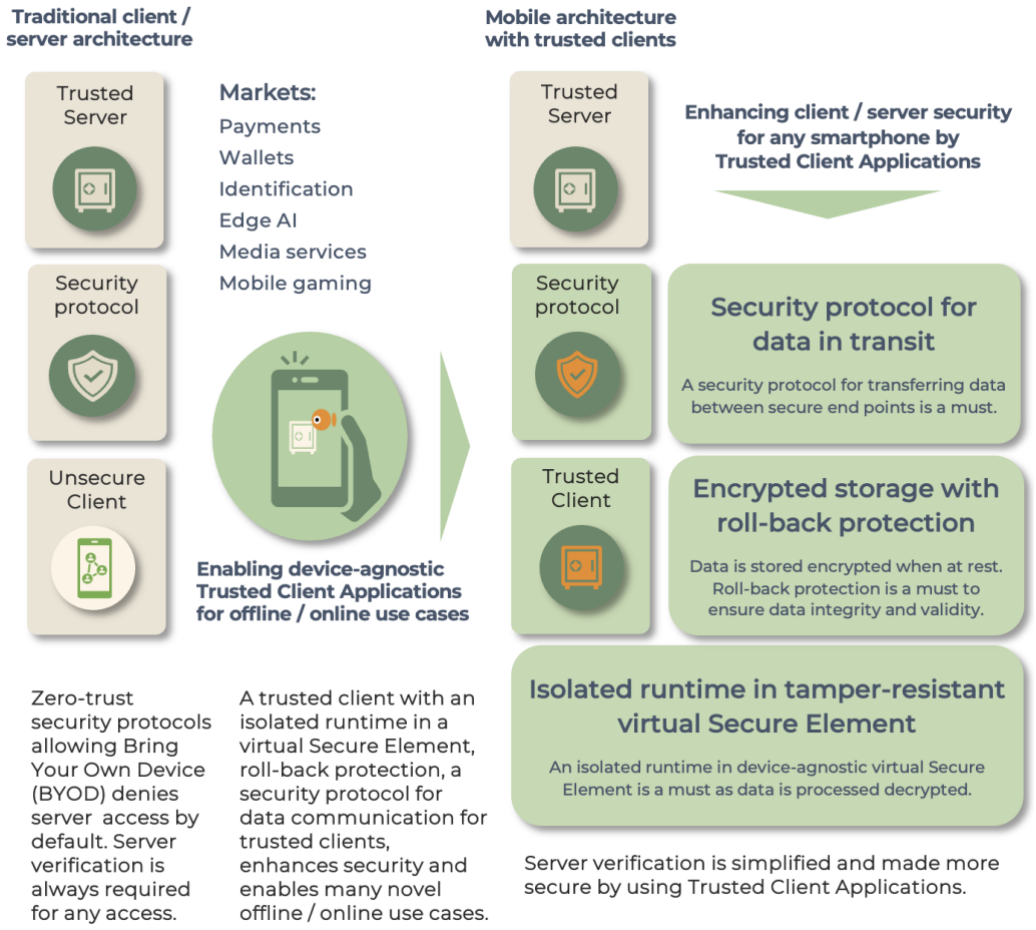

Figure: Enabling device-agnostic Trusted Client Applications for offline / online use cases across multiple market segments from mobile payments to AI edge computing

[4] https://www.v-key.com/wp-content/uploads/2019/07/V-OS-Virtual-Secure-Element-2022-3.pdf

Benefits of trusted client applications
Trusted clients in mobile applications provide multiple benefits that may be categorized as server enhancements, offline capabilities, system benefits and commercial benefits.

Server enhancements
The server can rely on the trusted client to perform certain security checks and validations locally before sending data to the server. This offers **increased security** as the attack surface and vulnerabilities that malicious actors could exploit are reduced. It is also possible to offload security checks and processing from the server, leading to improved performance, **load balancing** and scalability of the system. Furthermore, trusted clients enable **seamless authentication** and encryption integration within the client application, enhancing the user experience without compromising security. Trusted clients facilitate also secure end-to-end encryption between secure endpoints in the client and the server, ensuring confidentiality and data integrity.

Offline capabilities
Trusted clients can securely store and manipulate data locally before synchronizing and communicating with the server, providing **resilient service** and flexibility, and improved user experiences through **reduced latency**. Offline capabilities are also an important enabler for **user privacy**.

Figure: Trusted client applications provide multiple benefits to mobile client / server systems.

System benefits
The versatility and adaptability of device-agnostic trusted client applications allowing organizations to deploy many **novel use cases,** enable seamless scalability and **flexible deployments** by managing applications across diverse edge devices without device or platform dependencies. For industries subject to stringent data protection regulations offline processing capabilities offered by device-agnostic trusted client applications facilitate **regulatory compliance**. By ensuring that sensitive data remains on devices organizations can adhere to industry-specific regulations and data protection standards without compromising operational efficiency or data security.

Commercial benefits
By enabling offline capabilities present mobile application providers with many commercial benefits such as **new revenue** generating opportunities by offering offline as a value-added service, **improved service** competitiveness through enriched user experience and service differentiation, improved market reach by offering application service in new geographies, or higher service resilience in case of no connectivity or server congestion or temporary downtime as well as use cases requiring fast response times without any lag. Another key commercial benefit of trusted client application is that it **ensures licensing** despite applications rely on processing in the client rather than the server.

How important a particular benefit is depending on the market industry. and whether there already are existing trusted client solutions in place in the segment, such as Digital Rights Management within Media Services. The figure below describes the importance of the benefits for use cases within payments, wallets, identification, edge AI, media services, and mobile gaming.

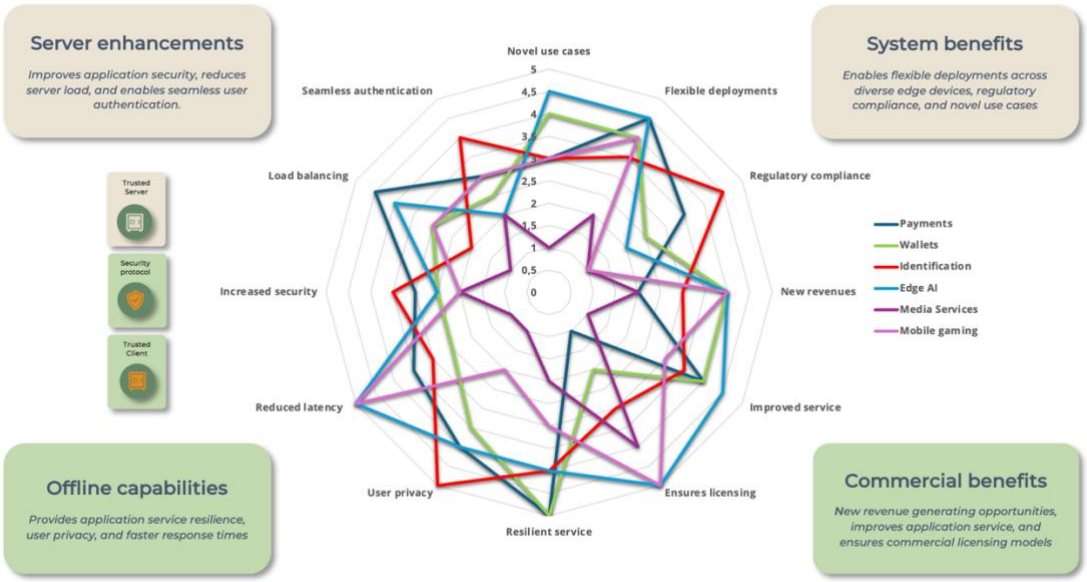

Figure: The importance of benefits of introducing trusted client applications to various market industries

The case for device-agnostic trusted client applications
Device-agnostic trusted client applications come with pre-packaged superior security for logic executing in the client. It provides an isolated runtime in a tamper-resistant virtual SE for offline data processing using cryptographic operations, encrypted storage with roll-back protection to ensure data integrity and validity and implements a security protocol for transferring data between secure endpoints to avoid man-in-the-middle attacks.

A common belief is that hardware-based SEs are always more secure than software-based virtual SEs because of the clarity of security boundaries. However, due to the inevitable separation between the payment app and the hardware-based SE, there is a gap in the chain of trust between the two communicating endpoints. This can result in potential attacks by replacing either endpoint with malicious ones or tampering with them and modifying their behaviors during runtime. As the hardware-based SE does not have full visibility of the payment app and the mobile OS, it cannot determine the identity of the app or whether the app has been tampered with, and must "blindly" trust the OS and the app.

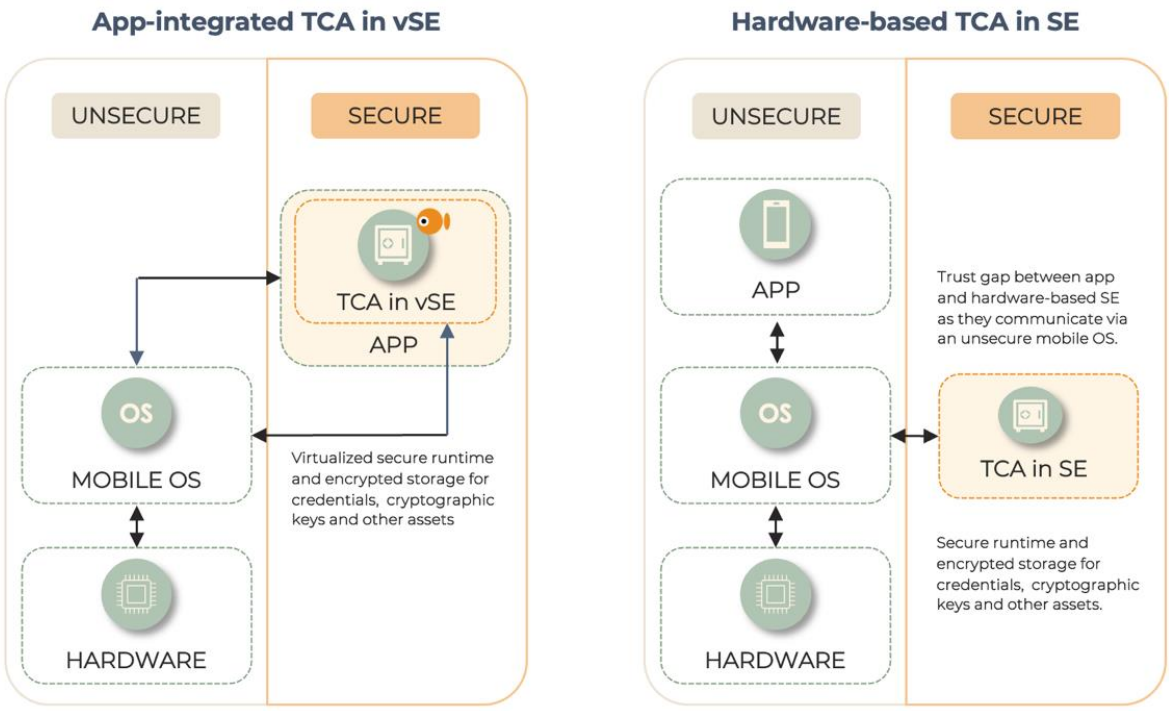

Figure: Device-agnostic trusted client application executing within an app-integrated virtual SE vs. trusted client application in SE with a trust gap between the app and the hardware-based SE as they communicate via an unsecure mobile OS.

There are multiple key benefits with a device-agnostic trusted client application implemented in a virtual SE that advocates of hardware-based SE solutions often fail to mention:

1. Device-agnostic trusted client applications are app-integrated and implemented in a virtual SE and has no costs associated with hardware or its physical distribution.

2. Dependencies on hardware-based SE always limit the addressable user base of the application as it can only be deployed to specific mobile devices.

3. There is no eco-system infrastructure available to provision trusted client applications with hardware-based SEs. A trusted client application in a virtual SE, on the other hand, is built into the mobile app itself and can therefore be distributed and upgraded as an integral part of the mobile app using standard eco-system for downloading apps on Google Play for Android applications and App Store for iOS applications.

4. When the trusted client application is device-agnostic and tightly integrated with the mobile app then there is no trust gap between the app and the trusted client in contrast to a trusted client in a hardware-based SE as it will always be separated from the app, which exposes the trusted clients for attacks from malware apps.

5. It is necessary to base the security on the assumption that rooted / jailbroken mobile devices exist in the market, where a potential attacker have full control over the mobile device including its mobile-OS and the files systems of the apps. Root detection software is simply not able to provide the required level of security. A device-agnostic trusted client application that is app-integrated, on the other hand, runs securely also on rooted / jailbroken device which is another key advantage.

6. It also necessary to assume that the system security will be compromised eventually. It is only a question of how long time it will take. The Bank of International Settlement reports that the average time it has taken to break the security in Decentralized Finance applications is 10 months only. In this case, it is important to be able to limit the security breach by isolating it to specific clients and for the system to have the ability to lock such clients when they go online or when their certificates expire.

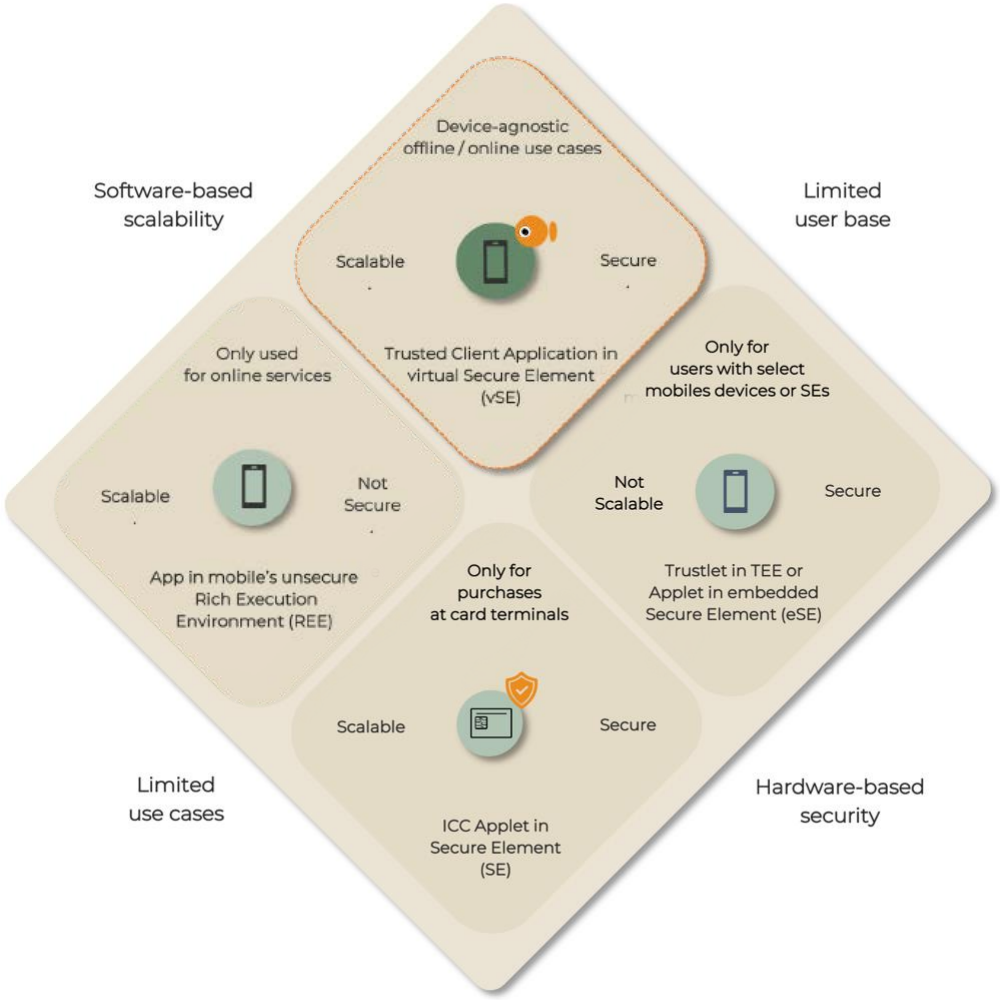

Figure: Overview of client architectures and their limitations. A trusted client application in a virtual SE is device-agnostic and supports all offline and online use cases. A mobile application using a hardware-based trustlet in a TEE and applet in an embedded SE, on the other hand, is not scalable as the mobile application is limited to users with select mobile devices or with access to specific hardware-based SE, such as a security key or a SIM card.

Implementing offline payments

Crunchfish has solved many technical challenges to enable offline payments and these technical innovations can be generalized to any mobile applications, even involving offline execution and storage[5]. It does not have to be a use case within mobile payment. It is all about how to implement device-agnostic trusted client applications. To understand the technical features of a device-agnostic trusted client application better these are first explained within the context of offline payments.

[5] https://www.crunchfish.com/crunchfish-patents-device-agnostic-trusted-client-applications-for-offline-use-cases/

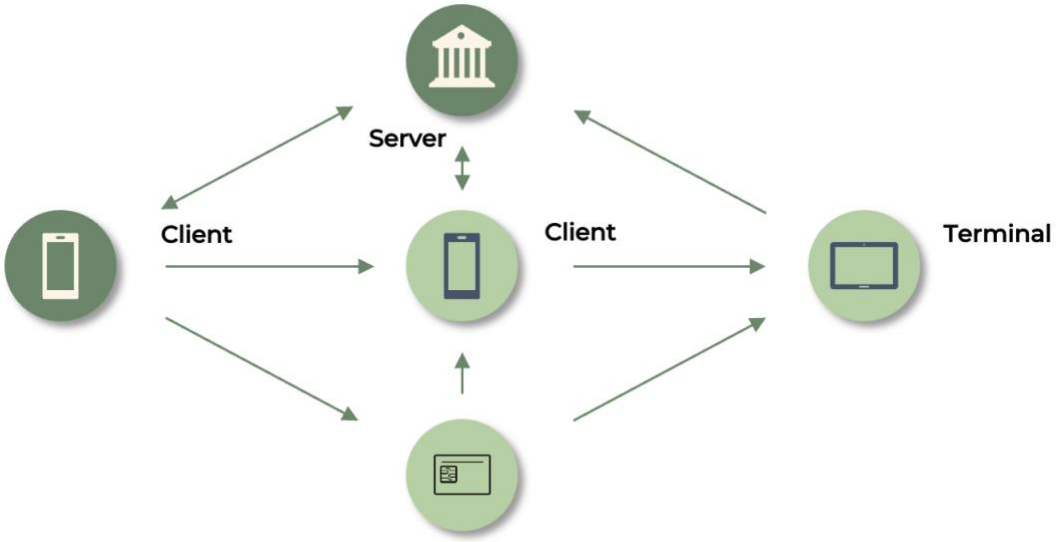

Figure: High-level architecture of an offline payment system. It involves client and server communication to fund / defund wallets and uploading transactions to the ledgers on backend servers. The offline transactions are client to client / terminal interactions. An offline payment system works by leveraging trust that has been established in the mobile clients.

Many mobile use cases outside of payments and wallets, for instance identification, edge AI, media services and mobile gaming involves client / server communication only. Many novel use cases can be realized with the ability place trust in the mobile clients.

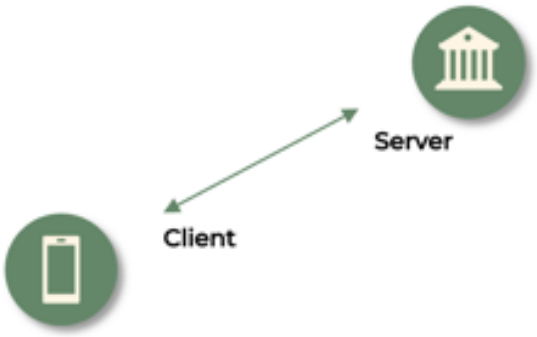

Figure: A mobile client / server system. In typical implementations the server where the application logic executes does not trust the mobile client. By establishing trust in mobile clients, the overall system security may be enhanced, and many novel use cases may be realized.

There are many technical features that must be implemented to enable device-agnostic trusted client applications. The below diagram displays the Security Impact vs. Development Complexity of such technical features. The features are colour coded to describe technical features that ensures trust in clients in mobile client / server systems in dark green and in light green the technical features that leverages trust between clients in client-to-client interactions. This is followed by two tables with short descriptions for each technical feature. As can be seen in the diagram, it is relatively easy to implement a specific Client Application Logic for a specific use case compared to developing the many technical features required for having trust in clients.

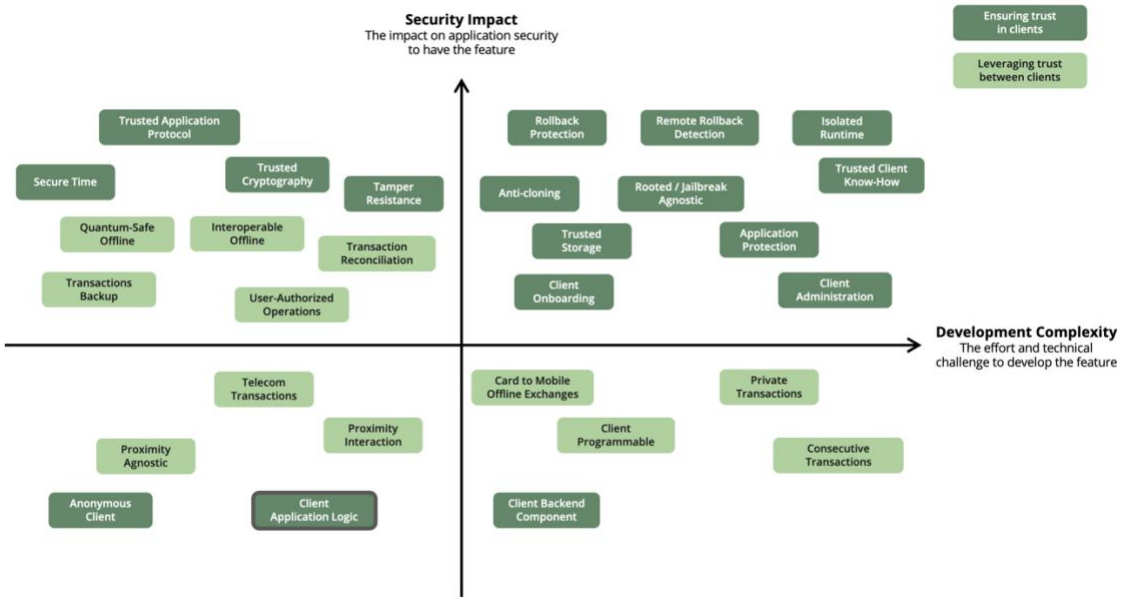

Figure: Security Impact vs. Development Complexity for technical features of device-agnostic trusted client applications

Crunchfish has patented many of the technical features for device-agnostic trusted client applications, especially for offline use case. In addition to improved security through roll-back protection[6], anti-cloning[7], quantum-safe[8] offline implementation and a Trusted Application Protocol[9] for data in transit that is agnostic-to-anything, also functionality such as privacy[10] [11] [12], interoperability[13] and responsive Bluetooth proximity interaction. Crunchfish offers trusted offline client applications that can be integrated within the app and is therefore deployable for all mobile devices. It has potential in many mobile client / server systems as trust in clients complements the trust offered by the server. This opens many novel use cases, both offline and online.

[6] https://www.crunchfish.com/crunchfish-patent-fraudulent-rollback-protection-of-trusted-applications/
[7] https://www.crunchfish.com/crunchfish-prevents-fraudulent-cloning-and-digital-cash-double-spending/
[8] https://www.crunchfish.com/crunchfish-receives-positive-patentability-report-for-quantum-safe-digital-cash/
[9] https://www.crunchfish.com/crunchfish-receives-positive-examination-report-for-strategically-important-digital-cash-patent-application/
[10] https://www.crunchfish.com/privacy-considerations-in-cbdc-systems-new-whitepaper-by-crunchfish/
[11] https://www.crunchfish.com/crunchfish-provides-and-patents-digital-cash-privacy/
[12] https://www.crunchfish.com/crunchfish-patents-anonymous-and-robust-trusted-applications/
[13] https://www.crunchfish.com/crunchfish-receives-clean-iprp-for-key-digital-cash-patent-application/

Feature	Description
Isolated Runtime	Secure execution environment designed to run Trusted Client Applications isolated from the rest of the system.
Remote Rollback Detection	Monitor and analyse offline transactions to detect if a client has reverted to a previous state.
Rollback Protection	Prevents files from being restored to a previous state, providing data integrity of the Trusted Client Application.
Trusted Application Protocol	All messages between entities are digitally signed which provides end-to-end integrity and validates the sender's identity.
Trusted Client Know-How	Expertise in the field of a Trusted Client Applications
Rooted / Jailbreak Agnostic	Allows execution on rooted or jailbroken devices without compromising security.
Anti-cloning	Ability to disallow multiple clones of clients in mobile client / server system
Tamper Resistance	Monitoring suspicious activities and attempts to tamper with the secure environment and if identified restricting access.
Trusted Cryptography	Ensures data security and privacy by performing cryptographic operations within the Trusted Client Application.
Secure Time	Reliable and tamper-proof clock that is protected from unauthorized adjustment.
Application Protection	Mechanisms protecting the mobile app from tampering.
Trusted Storage	Secure storage that ensures that data used by the Trusted Client Application is protected through encryption.
Client Administration	Allows the system to configure the rules and policies that governs the behavior of a client.
Client Onboarding	Locally initiate a client, apply personalization govern by the system and activate the client.
Client Backend Component	Simplified backend integration by handling the client communication and functionality.
Client Application Logic	**Logic targeting a specific client application use case.**
Anonymous Client	Onboarded client without KYC.

Figure: Technical features that ensures trust in clients in mobile applications.

Feature	Description
Quantum-Safe Offline	Quantum-safe offline transactions
Interoperable Offline	Interoperable cross-scheme and cross-border offline transactions
Transaction Reconciliation	Collect and verify client transactions from both the sender and the receiver independently.
User-Authorized Operations	Authorization by passphrase or biometrics before execution trusted client operations.
Transactions Backup	Backup client transactions to prevent them from being lost upon uninstalling the app.
Private Transactions	Ensures that the client transaction remains private and confidential.
Card to Mobile Offline Exchanges	Value exchanges between Trusted Client Applications on cards and mobile devices.
Telecom Transactions	Transferring of data between an app and the backend relying on the telecom network.

Consecutive Transactions	A series of data exchanges between clients in proximity without relying on network connectivity.
Client Programmable	Leverage the power of handling multiple containers each with its own individual rules for making client transactions.
Proximity Interaction	Transferring of data between clients in proximity without relying on network connectivity.
Proximity Agnostic	Operates seamlessly with various proximity technologies as a medium for offline transactions between clients.

Figure: Technical features that leverages trust in clients in client-to-client interactions.

Implementing Edge AI

The proliferation of artificial intelligence (AI) applications at the edge has catalyzed the need for secure offline data processing capabilities to ensure data privacy, compliance, and reliability in sensitive environments. Device-agnostic trusted client applications play a pivotal role in facilitating offline data handling for AI applications, offering a versatile and secure platform for processing sensitive data at the edge. The tables below outline benefits for AI use cases that involve handling sensitive data offline in the clients.

Benefits	**Rationale**
Data Privacy and Security	Device-agnostic trusted client applications bolster data privacy and security by enabling offline data processing, reducing the risk of unauthorized access or data breaches associated with continuous connectivity to the cloud. By processing sensitive data locally at the edge, organizations can maintain stringent security controls, encrypt data at rest, and implement access permissions to safeguard critical information from external threats.
Regulatory Compliance	For industries subject to stringent data protection regulations, such as healthcare, finance, and manufacturing, offline processing capabilities offered by device-agnostic trusted client applications facilitate compliance with regulatory requirements. By ensuring that sensitive data remains within the organization's control, organizations can adhere to industry-specific regulations (e.g., GDPR, PCI DSS) and data protection standards without compromising operational efficiency or data security.
Reduced Latency and Reliable Connectivity	Offline data processing at the edge with device-agnostic trusted client applications enhances AI application performance by reducing latency and ensuring reliable connectivity in environments with limited or intermittent network access. By processing data locally, organizations can enhance real-time decision-making, improve system responsiveness, and mitigate disruptions caused by network latency or connectivity issues, thereby optimizing operational workflows and user experiences.

Scalability and Flexibility	The versatility and adaptability of device-agnostic trusted client applications enable seamless scalability and flexibility in AI deployments, allowing organizations to deploy and manage AI applications across diverse edge devices without platform dependencies. By supporting offline data processing capabilities, organizations can scale their AI initiatives, deploy updates or new features efficiently, and adapt to changing business requirements while maintaining data security and privacy standards.

Industry	**Use cases**
Generative AI	A device-agnostic trusted client application that can operate independently from the server enhances generative AI systems by providing improved responsiveness, privacy, offline functionality, customization, resource efficiency, and edge computing capabilities. Such a setup can lead to a more robust, flexible, and user-centric AI experience across various devices and network conditions. Furthermore, trusted clients protect commercial licensing models and can also provide new revenue opportunities. Offline operations user experience, revenue growth, and business sustainability for mobile application providers in the competitive mobile AI app market.
Financial services	The financial services sector demands robust security measures for handling sensitive financial data in AI applications such as fraud detection, risk assessment, and personalized banking services. Device-agnostic trusted client applications provide a secure offline environment for processing financial data at the edge, enhancing data protection, mitigating cybersecurity risks, and enabling real-time analytics without compromising privacy or confidentiality.
Industrial Internet of Things (IIoT)	In industrial settings, where sensitive operational data from machinery and sensors powers predictive maintenance, asset optimization, and process automation, device-agnostic trusted client applications enable offline data processing for IIoT applications. By processing sensitive data locally at the edge, industrial organizations can improve operational efficiency, minimize downtime, and ensure data integrity while adhering to strict security protocols and operational continuity requirements.

Conclusion

Device-agnostic trusted client applications are indispensable tools for enabling secure offline data processing in mobile applications for a diverse range of use cases from mobile payments to edge AI. Trust in clients requires a robust framework for handling sensitive data across diverse industries and one aim of this whitepaper has been to point to the diverse set of technical features required. By harnessing trust in clients in mobile applications, organizations can have multiple benefits that has been described as server enhancements, offline capabilities in the clients, system benefits, and commercial benefits in systems that involve processing sensitive data offline. As the demand for secure offline solutions continues to grow, the integration of device-agnostic trusted client applications will play a pivotal role in fostering innovation, security, and reliable operation for many use cases across many industries.


crunchfish
TRUST IN CLIENTS