COEXISTENCE OF NFC APPLICATIONS

On Android Handsets

EXECUTIVE SUMMARY

Mobile payments are currently being adopted across the world at a rapid pace, with new Near Field Communication (NFC) applications emerging in quick succession. These apps are developed independently from one another. With the increasing number of available NFC applications, the chance of coexistence problems also increases. We consider something a 'coexistence problem' when the behaviour of one NFC service negatively affects an NFC service of another Service Provider.

Due to the complexity of the NFC domain, we will break it down into three environments. Based on these environments, we will cover the details of the most relevant technical background information and discuss the challenges for the parties involved. Finally, we will explain how these challenges can be tackled by NFC service providers and Secure Element issuers.

This white paper will focus on NFC payment services at a point of sale (POS) for Google's mobile operating system Android. This will not include the provisioning process of a digital card or peer-to-peer (P2P) transactions.

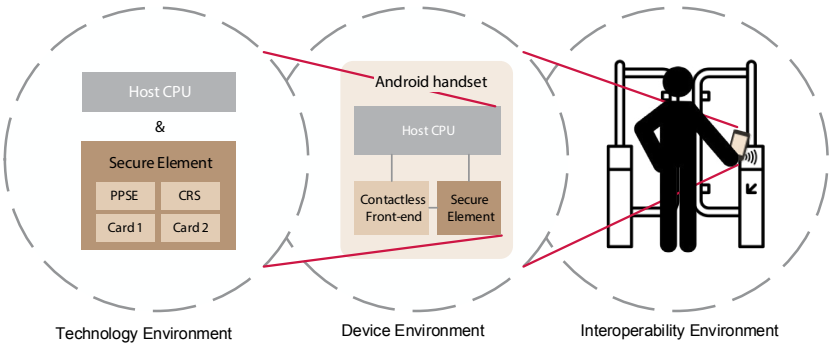
COEXISTENCE OF NFC APPLICATIONS

On Android Handsets

COEXISTENCE ENVIRONMENTS

Three environments have been identified where coexistence problems may occur:

1. Technology environment
2. Device environment
3. Interoperability environment



1. TECHNOLOGY ENVIRONMENT

The 'lowest' level where coexistence problems can occur is in the technology environment. This is the location where NFC applications live, which can either be a Secure Element (SE) or the host CPU (see sidebar). When multiple payment cards use the same technical environment, problems may occur when deciding which card should be used when presented to a payment terminal. For host applications, this decision is made by the application itself, while for the SE, the Contactless Registry Service (CRS), as defined by GlobalPlatform, is responsible.

2. DEVICE ENVIRONMENT

A single device can contain multiple technology environments. These different technologies have to work together within the device environment. Coexistence problems may occur when multiple NFC applications, using different technologies (UICC, eSE or HCE), exist on the same mobile device. As there are various ways of prioritizing NFC applications, experience shows that it is a challenge to set them up in such a way that they always work as expected. In order to control this behaviour, Android uses a routing table to define which virtual card should be used for a transaction.

NEAR FIELD COMMUNICATION

Near Field Communication (NFC) is a technology that allows wireless communication between two devices over a short distance (~10cm). The security of NFC data transactions is traditionally based on a Secure Element (SE). This is a tamper resistant chip inside the handset which can perform cryptography functions and store sensitive data.

There are three types of SEs: Universal Integrated Circuit Card (UICC), embedded Secure Element (eSE) and micro SD. A UICC is an advanced SIM card, owned by a Mobile Network Operator (MNO). An eSE is an integrated component of a phone's hardware and owned by a mobile device manufacturer (OEM). A micro SD is not commonly used for NFC services.

With the introduction of Android 4.4 Kitkat, Google introduced a software based alternative for SE: Host-based Card Emulation (HCE). Instead of routing data to a SE, the NFC controller routes the data to the CPU (Central Processing Unit) inside the phone, on which Android applications are running. This allows service providers (SP) to offer NFC payment services without having to rely on other parties to provide an SE.

3. INTEROPERABILITY ENVIRONMENT

In order to successfully perform NFC transactions, the mobile device will have to interact with a terminal. We call this the interoperability environment. On this highest level, coexistence challenges may occur when different devices interact. For standard payments and interoperability testing on this level, UL has published a separate white paper[1]. In some countries it is already possible to use a mobile device for both public transport and mobile payments. When hardware such as transit gates supports both public transport and payment solutions (EMV in transit), additional coexistence problems problem may occur. This phenomenon, which is called card clash, is covered in the Challenges section of this paper.

TECHNICAL BACKGROUND

Before going into detail about the coexistence challenges, we will cover three technical topics, each relating to a different environment. The topics are Contactless Registry Service (technology environment), Android routing (device environment), and ISO 14443 (interoperability environment).

1. CONTACTLESS REGISTRY SERVICE GOVERNANCE

For SE based solutions, a critical element influencing the routing behaviour inside the SE is the Contactless Registry Service (CRS). The CRS manages which contactless applet is advertised to the NFC controller on the handset, and indirectly to a contactless terminal. For payments specifically, the CRS manages which payment card, together with the Proximity Payment System Environment (PPSE), is advertised to the NFC Controller and indirectly to a POS. A GlobalPlatform compliant SE allows multiple Service Providers (SPs) to provision their service on the same SE. During service usage, a Secure Element Issuer (SEI) has several options to govern how each SP can enable and disable its payment cards in the CRS towards the NFC Controller of the device.

To ensure that only one payment card with a corresponding individual Application Identifier (AID) is presented by the PPSE, changes in the status of any enabled payment card by another SP payment application should result in conflicting payment cards being disabled in the PPSE, as otherwise multiple cards with the same AID can be presented simultaneously to the POS. Traditionally, a SEI wallet took care of this process. However, when each SP has its own application with access to the CRS, the process becomes more complicated, as the SP now has to modify the activity of other payment applications as well. The amount of freedom a SP application has to manage the contactless availability of applets via the CRS is decided by the SEI. There is no cross-industry standard on how to manage the contactless availability of payment cards on a SE.

2. ANDROID ROUTING

To ensure that a terminal interacts with the correct NFC card on a handset, the NFC controller on a handset uses a routing table. This table is populated with the PPSE, the AID of the available cards, and in which technology environment they are located. The PPSE is an application responsible for describing which payment applications are available to a POS. Every digitized card has an AID, which is a unique application identifier per technology environment.

Users can decide the order of the NFC cards in the routing table through a settings menu called “Tap & Pay”. This menu offers the following functions:

- **Payment default:** This menu allows the selection of a default payment service. This is the payment application that is launched by Android when an NFC event for a payment transaction arrives. Note that all payment transaction events are routed to the default payment application.

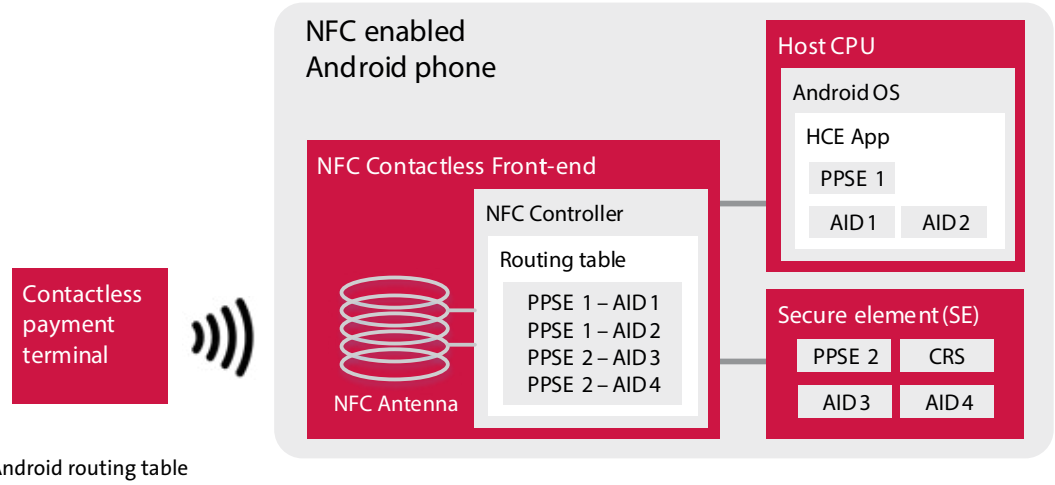


Figure 2: Android routing table

[1] To download the white paper, please visit the Knowledge Sharing section at UL-TS.com.

- **Use default:** This option allows users to indicate when they want to use the default payment application. Users can indicate whether they always want to use the default application or that they want to favour another payment application to be used when it is opened and displayed on the foreground.

If users have multiple payment cards belonging to a single bank, they have to select their preferred payment card inside the payment application. Theoretically, it is also possible to arrange this via the Tap & Pay menu. However, that would result in the same logo and description appearing multiple times in the Tap & Pay settings menu, making it very hard for users to distinguish the payment cards.

Figure 3 provides an example of the decision path for users, when selecting an NFC card on a mobile phone. In this example, three payment applications are installed with each using a different NFC technology (HCE, UICC, and eSE) and containing two payment cards.

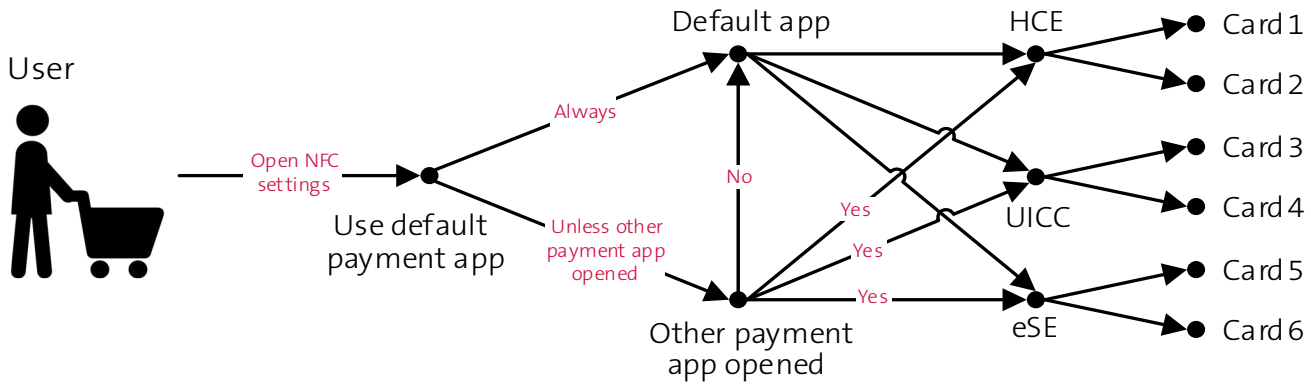


Figure 3: User decision tree when selecting an NFC card

In order for a payment service to access a device's NFC hardware and appear in the Tap & Pay settings, it has to be declared in the Android Manifest. Every Android application must have an AndroidManifest.xml file. In this manifest, the payment application needs to declare an APDU service including: the NFC technology (HCE or SE), supported AIDs, type of NFC service (payment or other), and an icon for the Tap & Pay menu. When it concerns a Host Card Emulation (HCE) application, the manifest also has to declare whether it can be used when the phone is unlocked.

3. ISO 14443

IISO 14443 is a set of transmission protocols for communicating with contactless proximity cards. It is divided into four layers: physical characteristics (14443-1), radio frequency and signal interface (14443-2), initialization and anti-collision (14443-3), and transmission protocol (14443-4).

ISO 14443 defines two types of cards, Type A and Type B. Both cards operate with a 13.56 MHz electromagnetic field and use the same transmission protocol (14443-4), but the modulation mode (14443-2), initialization procedure (14443-3), and protocol activation (14443-4) are different between Type A and Type B cards.

Near Field Communication defines the communications between two devices over the contactless interface. It is based on ISO 18092 and ISO 21481 and is backwards compatible with ISO 14443-2 and 14443-3 for Type A and B contactless cards. It defines a different command protocol to replace ISO 14443-4. As it only supports ISO 14443-2 and 14442-3, NFC also dictates a different antenna size.

In addition to NFC, ISO 14443 is also used for other popular contactless interfaces, such as EMV (for payments), MIFARE (for transit and access control), and Calypso (for electronic ticketing). Although these implementation are based on the same standard, it they are not fully interoperable. EMV, for example, is based on all four parts of ISO 14443 - and even defined a 5th layer on top. On the other hand, MIFARE (Classic) only uses the first three ISO 14443 layers in combination with a proprietary transmission protocol.

CHALLENGES

The number of variables and implementation specifics that need to be taken into account when implementing NFC solutions make it difficult to ensure that an application exhibits consistent behaviour. Four major challenges have been identified which will now be elaborated.

1. CONVENIENCE

A claim that is often used to promote mobile payments is 'convenience'. But is it really convenient to use mobile phones for contactless payment?

First, users have to be aware of the differences in behaviour between HCE and SE. HCE can only be used when a mobile phone's screen is turned on, while for SE the screen can be on or off. As a result, it can occur that a user selects an HCE payment app as default, but pays with a SE based payment app as the phone's screen was off during exchange of data with the POS.

Another aspect that can be confusing for users is the Tap & Pay settings. When only one payment application is on the device, it is automatically selected. However, when multiple NFC applications exist on the same device, it is a different story. Users have to select their default app, but also which app should be used when it is opened (on foreground). Furthermore, every individual bank must implement a process for users to decide on a default NFC card when multiple are present in the same payment application.

2. BEHAVIOR CONFIGURATION OF THE SE BY OTHER PARTIES

Although the majority of implementations going live on Android handsets nowadays are HCE based, a number of arguments still support SE use. With SE, the security model is easier. Also the PIN entry experience for the user is more intuitive as the SE can verify the PIN for all payment schemes.

However, the main problem for SE solutions is that the SE is typically owned by a different entity than the service provider. Traditionally, the SEI provides a 'wallet' application. This ensures correct when multiple service providers have an applet installed on the SE. In practice we see that many service providers prefer to have their own payment application, in order to fully control the branding of and customer experience with the application. In the absence of a wallet with rights to (de-)select all applets, interoperability issues can occur when there are multiple applets active on the SE simultaneously.

3. CARD CLASH

The majority of payment and public transport terminals use an implementation based on ISO 14443 to communicate over the contactless interface. As NFC is also based on this protocol, ISO 14443 allows NFC-enabled phones to communicate with contactless terminals.

EMV is the ISO 14443 implementation most used for contactless payments; for transit, leading implementation concern MIFARE, Calypso and FeliCa. Traditionally, EMV was only used in the payment domain, but some Public Transport Operators (PTO) have now adopted "EMV at the gate". This allows travellers to travel both with their transit card and mobile payment application.

When all standards are implemented correctly, this should not impose any problems unless a bank card and transit card are presented simultaneously. As the gate is constantly polling for both cards, it is unclear to the device and the user which card should be selected due to the random nature of the resolution for this issue defined in ISO 14443. With physical cards, this issue can easily be solved by taking one card out of the wallet and presenting it to the gate. With NFC cards on a mobile phone, card selection becomes more difficult. As it is possible for a payment card and a transit card to be active on a mobile phone at the same moment, the gate will use a vendor-specific way to decide which card to select, thereby risking that the wrong card is selected. Also, there is no menu in the Android operating system that allows users to prioritize an EMV card over a transit card.

RECOMMENDATIONS

We have discussed the different environments that need to be taken into account when optimizing the customer experience. Unfortunately, these are often controlled by different (sometimes even competing) entities. What should each party in the ecosystem do in order to ensure the best experience for their users? What pitfalls should be avoided?

1. INDIVIDUAL SERVICE PROVIDERS

Correct technical implementation: First of all, SPs must ensure they have a technically correct implementation that provides proper interoperability at both handset and application level. It is therefore important to follow the Android guidelines on registering applications for the required notifications in the manifest file. This prevents issues at the application level and reduces the issues at the handset level.

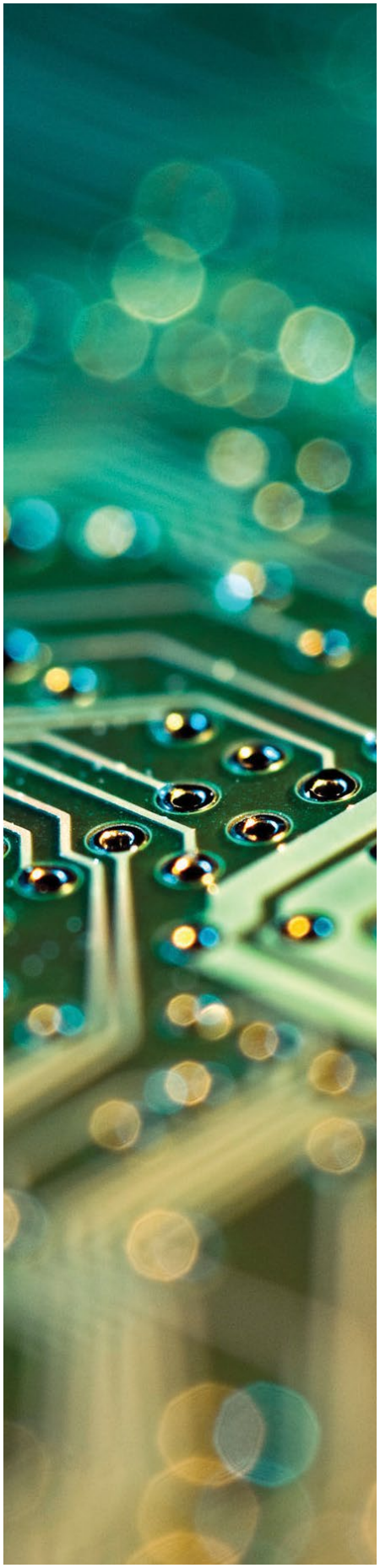
Educate the end user: Even when all unexpected behaviour is solved from a technical perspective, unwanted behaviour can still appear unexpectedly to the end user. For example, at the handset level the Tap & Pay settings are hidden and unintuitive for many consumers. It becomes even more complicated with the possibility to prioritize a foreground app or the Advanced Tap & Pay Settings (introduced by Samsung). In an ecosystem where this is not handled intuitively it is wise for the SP to try to educate the consumer on the location and meaning of the different settings. With many handsets, firmware versions, NFC technologies, applications, and settings, SPs should help customers in setting up and using their services.

2. SECURE ELEMENT ISSUERS

Contactless Registry Service (CRS) Governance: To make sure that only a single payment application and corresponding AID is presented to the POS terminal in the PPSE, the CRS needs to enable the correct applet. When SPs are allowed to have their own payment application (independent of a SEI wallet) there are several options available. The following list contains implementation options that have been observed in the field alongside hypothetical (but realistic) ones. The list is ranked from most amount of freedom for SPs, to least amount of freedom.

1. No access restrictions for SPs, and no SEI policy on how to interact with the CRS.
2. No access restrictions for SPs to the CRS, but a SEI policy is in place regarding usage of the CRS and how applets outside the SP's domain should be handled.
3. No CRS access restrictions for SPs, but the SEI implements an extended CRS and specifies how SP applications shall use this extended CRS.
4. Access from SPs to own applets only, thereby requiring applets to be installed with self-activation privileges.
5. Require SP applications to use inter-app APIs towards a SEI app on the handset to request contactless activation/ deactivation of an SP applet.

Each option has its own interoperability and security advantages and disadvantages. For each SEI



implementation, the best solution will be a balance between ease of implementation, user experience, and security. An absence of CRS access restrictions yet adherence to a SEI policy (option 2) results in the least friction during payment service implementation and use. Such an option could prevent SPs to accidentally disable applets belonging to other SPs nor does it force them to use special privileges or a proprietary, not standardized CRS solution. One security drawback for this option is that SPs can see which other applications are installed on the SE and potentially enable or disable these applications.

3. JOINT EFFORTS

Collaborate: This white paper shows that a proper implementation from a single SP does not guarantee that its service works as expected. A bad implementation from one company can have detrimental effects to a different implementation. Even though it might not be your concern if a competitor's service does not work as desired, one application malfunction in the ecosystem can result in customers losing faith in the entire ecosystem. It is therefore essential that even competitors collaborate on a technical level to avoid interoperability issues.

When parties with (potentially) conflicting interests collaborate, it often proves difficult to reach consensus on who to solve the problem. Hiring an independent party that all ecosystem participants trust can be of great benefit to solve any issues. On the application and handset levels a trusted party could verify the coexistence of multiple (reference) applications on a number of market-representative devices. On a service level, interoperability testing with a set of (reference) terminals could be performed.

Correct technical implementation: Unfortunately, it is not possible for SPs to fully eliminate issues at the handset level, e.g. the NFC controller capabilities and behaviour depend on the NFC controller chipset version, firmware version, and even driver version. These can only be resolved by the handset manufacturer. If issues persist even when the SP has implemented everything correctly, the OEM should be contacted. As this can be a challenge for individual SPs, a payment scheme or independent third party that is trusted by both SP and OEM should be consulted.

For the service level, the technical implementation will often depend on handset and terminal manufacturers. Involving such parties is the best approach, but can be challenging due to their size.

Define a policy to support multiple protocols: When a single terminal supports multiple communication protocols, both EMV and MIFARE, SPs (PTOs) should clearly define a policy how the terminal should interact with those dual interface cards. This should be done with a representative reflection of the ecosystem, involving all involved parties: SPs, SEIs, OEMs and terminal suppliers.

SUMMARY + CONCLUSION

The mobile ecosystem is becoming increasingly complex. Many device models, operating system (OS) versions, NFC technologies, and different implementations make for a system that is constantly evolving. Successfully navigating this ecosystem is a challenge and a good understanding is needed to make the right decisions.

Each card issuer wants its solution to be regarded as the one-stop shop for mobile payments. However, with such competition, multiple SPs are fighting for dominance in the market. An incorrect implementation by one SP can impact others that have an application installed on that same handset. This results in the customer accidentally paying with a different application than expected. This is detrimental for a customer's trust in mobile payments. It is therefore essential that the competitors collaborate in achieving a proper and consistent user experience.

Such collaboration between competitors is tough but can be facilitated by standardizing the mobile payment solutions via the domestic payment associations or a global bodies (such as EMVCo). Collaboration become even more complicated if parties do not have an established trusted relationship. In these situations, there will be no joint governing body, e.g. if next to mobile payments a loyalty or transit NFC application is installed on the handset. The best solution is therefore the support of an independent party with expert knowledge across SPs.

For further information on NFC applications and mobile payments, please contact: **TRANSACTIONSECURITY@UL.COM** or visit **UL-TS.COM**

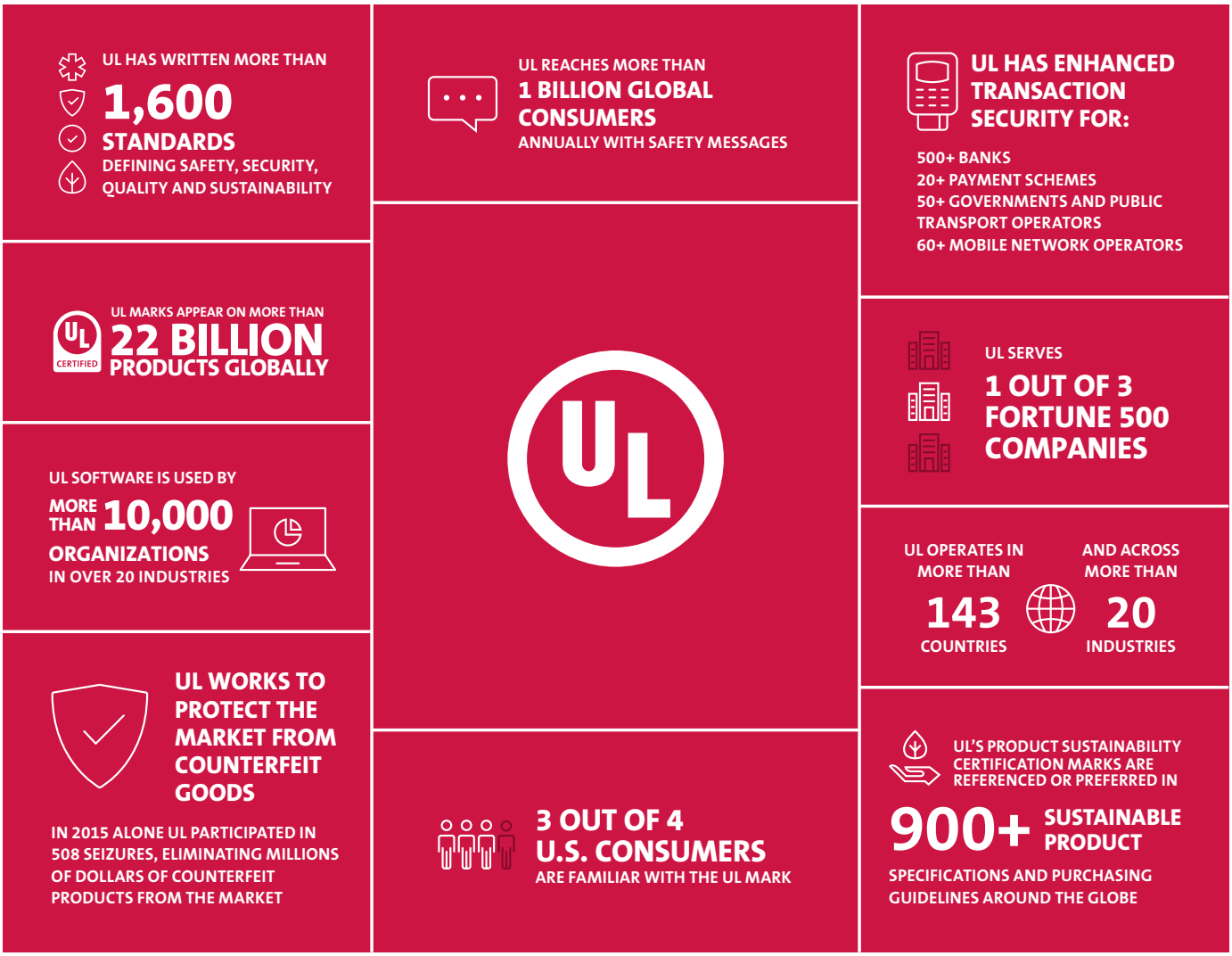
ABOUT US

UL fosters safe living and working conditions for people everywhere through the application of science to solve safety, security and sustainability challenges. The UL Mark engenders trust enabling the safe adoption of innovative new products and technologies. Everyone at UL shares a passion to make the world a safer place. We test, inspect, audit, certify, validate, verify, advise and train and we support these efforts with software solutions for safety and sustainability.

UL's Transaction Security division guides companies within the mobile, payments, and transit domains through the complex world of electronic transactions.

UL is the global leader in safeguarding security, compliance, and global interoperability. Offering advice, training, compliance and interoperability services, security services, and test tools, during the full life cycle of your product development process or the implementation of new technologies.

UL's people proactively collaborate with industry players to define robust standards and policies. Bringing global expertise to your local needs. UL has accreditations from industry bodies including Visa, MasterCard, Discover, JCB, American Express, EMVCo, UnionPay International, PCI, GCF, GlobalPlatform, NFC Forum, and many others. To learn more about us, visit UL-TS.com.



UL-TS.COM