Wearables to Weather: NXP's Innovations for a Secure and Smarter Future

From rockets in the air, to cars on the road and the cards in your wallet, our innovations at NXP have been integral to America's past and the success it enjoys today. As important as that legacy is, however, we at NXP are looking to the future and building a better, easier and safer tomorrow with exciting, leading-edge technologies of the utmost quality.

This is no small task. The rapid expansion of public and private data networks, the rise of social media and the mass deployment of smart objects across the Internet of Things, or IOT, have connected us in ways we didn't think possible two decades ago. They've also left us open, vulnerable and exposed.

To counteract these vulnerabilities, NXP is focused on:

- Avoiding unauthorized access in public and private areas of the IoT,
- Developing tamper-resistant secure element devices, and
- Perfecting the end-to-end solutions that power the new, often wearable technologies we'll use to improve and simplify healthcare, entertainment, transportation and the rest of our everyday lives.

Table of Contents

1 **Overview**

2 **No authentication? No access.**

2 **Personal and Public Security**

2 **"Bulletproof" Authentication**

3 **NXP's Secure Elements**

3 **NXP: Authentication Partner**

4 **What's Next in Wearables**

4 **Today's Wearables, Tomorrow's Next Big Things**

5 **NXP and the Wearable Future**

5 **The NXP Difference**

No authentication? No access.

Online security can mean different things to different people, but the tasks of keeping data private and ensuring cyber safety essentially come down to one thing: **access**. Whenever there's a failure in security due to a data breach, a denial-of-service attack, identity theft, the spread of malware, or some other act of sabotage, the failure can almost always be tied to unauthorized access. At some point, someone found a way to be where they shouldn't have been, and did damage.

At its core, maintaining security is about preventing unauthorized access, and that means verifying the identity of anyone or anything requesting entry. Before being allowed to submit data, modify information, save settings, or execute tasks, a person, a device, or a piece of software must first verify that they are who they say they are. This process, known as **authentication**, is the starting point for all online security. When done right, authentication protects every interaction, and makes it safer for people, devices, and applications to access and share data. In the purely cyber realm, where operating systems and software code can interact on their own, effective authentication prevents intrusions, thefts and attempts to introduce viruses or malware. There is no better way to ensure the effectiveness of security protocols than to require people, devices and software to present a trusted identity.

Personal and Public Security

No matter what the online scenario, authentication plays an essential role in keeping the process secure for everyone involved. For people using computers, smartphones, wearables, smartcards and electronic IDs to access services and exchange information, effective authentication ensures privacy while making purchases, logging onto a corporate network, riding public transport, updating health records, using government services, or simply sending an email.

In addition to individuals, industry and the government are often exposed to risk. For example, in his confirmation hearing, Ashton Carter, United States Secretary of Defense, stated that the Defense Department's network security "is not where it should be . . . [w]e're not anywhere near where we should be as a country . . . [n]ot only is our civilian infrastructure susceptible to cyberattack, but we have to be concerned about our military infrastructure."[1] For the rapidly growing IoT, effective authentication prevents criminals from accessing the data collected by devices or the software used to control device activity. This protects against the kinds of sabotage that can cripple the public infrastructure, which increasingly relies on smart grids and other network-controlled operations, and makes the IoT a safe place for private users, from the individual homeowner using a remotely-controlled thermostat to the global corporation or government managing thousands of connected devices.

"Bulletproof" Authentication

Essentially, authentication is the manipulation of secret information through cryptographic algorithms to ensure security. The main challenge to effective, even "bulletproof," authentication is the aging of authentication algorithms. Previously secure systems become vulnerable as hackers and other criminals begin to erode the protection mechanisms. Data that was safe yesterday may not be safe today or tomorrow.

Staying ahead of the curve in terms of authentication involves two things: optimizing the algorithms to make them stronger, and creating better ways to protect the authentication process. The goal is to keep the data used for authentication inaccessible.

1. Yuhas, A. (2015). Pentagon pick Ashton Carter discusses Iraq and Ukraine at Senate hearing – as it happened. *The Guardian*. Retrieved from http://www.theguardian.com/us-news/live/2015/feb/04/ashton-carter-senate-armed-services-committee-live.

NXP's Secure Elements

There are two aspects of authentication – the algorithms themselves and secure elements—tamper-resistant chip-based platforms that securely host an authentication algorithm and its confidential data. NXP's research indicates that in nearly all serious data breach cases, attackers extracted keys or credentials from devices or systems that offered no resistance. Our secure elements build on our groundbreaking work in microcontroller design, feature onboard countermeasures to protect from invasive, external attacks geared at data extraction, lead the industry in shipments and have earned a reputation for being many times more secure than their nearest competitors. For example, **NXP produces chips that have their own unique fingerprint, based upon their crystalline structure, so no two chips are alike, preventing cloning.**

NXP: Authentication Partner

NXP has made authentication a top priority for more than 20 years, and has continually reached new levels of performance by making algorithms more resilient, and by increasing the robustness of secure elements. We are a recognized leader in authentication, known for our ability to deliver trusted security in many of the world's most high-profile applications.

NXP's strength in authentication is closely tied to eGovernment and banking. With a roughly 80 percent share of the electronic passport market, our technology is trusted by more national governments to increase security while reducing wait times at international borders. We are helping governments expand the use of electronic documents, and our repeated successes with large-scale implementations for electronic IDs, public transport, and multi-application cards (which combine payment, transport, identification, and other services on a single card), make us a trusted partner to municipalities, transit authorities, and banking and payment organizations worldwide. NXP brings a comprehensive set of skills to each authentication challenge and leverage long-standing relationships with a broad spectrum of security leaders to deliver tailored solutions that address the particular needs of each application.

Now that you've seen how NXP will keep the future of connected devices secure, let's take a look at the forefront of these connected technologies, their possibilities, and NXP's current and future role in developing and securing this tech for a brighter future.

e-Government Applications

ELECTRONIC PASSPORT

Increased international border crossing security and efficiency

- Higher security
- Global Interoperability
- ICAO compliance
- Automated border crossing

NATIONAL ID

Provide electronic identification & enable governmental services

- Higher security for personal authentication
- Service cost and efficiency

HEALTHCARDS

Reduce healthcare costs via improved and efficient services

- Patient identity
- Electronic health records
- Medication management
- Enable social security services

What's Next in Wearables

Kazou Kashio, the CEO of Casio, was quoted not long ago describing the human wrist as "prime real estate." Kazou was alluding to the biggest technology battle that will take place in the next few years: the fight to dominate the wearable technology market. While there are a number of innovations taking place in the wearable technology space at the moment, with everything from smart glasses to intelligent hearing aids being developed, the competition probably will be fiercest around the wrist.

Previously, wristwear belonged exclusively to traditional watch manufacturers. Now technology companies are taking an interest in that "prime real estate" with the release of products like smart watches. Glancing down at a screen attached to the wrist is already such a natural action for many people. It's the reason why fitting someone's wrist with the latest tech in smart watches is so attractive for users and technology companies. While consumers will take some time adapting to devices such as smart glasses, strapping on the latest smartwatch is already seen as more of an upgrade that seamlessly blends smartphones and watches.

This evolution in wearable tech is all about enhancing users' lives and making everyday functions simpler and easier so we can concentrate on the things that matter. NXP creates the security, connectivity, and circuitry solutions that enable these wearables devices, their convenient applications in today's society and the innovative ways they could be used in the future.

It's All in the Wrist

Today's Wearables, Tomorrow's Next Big Things

To date, we've seen many smartwatch and other wrist-based innovations designed around fitness, health monitoring and entertainment. For example, Nike's FuelBand, the Fitbit and Jawbone products track steps, monitor heart rates and keep tabs on other vital information, all while synced to other smart devices.

Today's latest wrist-based tech innovation is not just limited to smartwatches. Walt Disney Parks and Resorts has unveiled its own RFID wrist tag application, the MagicBand. Walt Disney Parks and Resorts' MagicBands and cards are all-in-one devices that serve as guests' park tickets, room keys and more. The technology enables guests to book places on rides with the enhanced FastPass system FastPass+. RFID bracelets like the Disney MagicBand are increasingly being used for entrance and paying at other events with the tap of a wrist. It's simple, convenient movement that means no more lost cash at festivals.

NXP and the Wearable Future

There are already many existing areas where smart watches could improve users' lives. Today's keyless entry for vehicles will probably move to a wearable platform, and in the future, watches will act as the key for the entire car. In fact, most luxury car makers already offer their own wrist watches. It's a great channel to help build brand recognition.

In the home environment, smartwatches will interact with communications protocols such as ZigBee and Bluetooth®, allowing users to control the home environment. Heating, lighting, AV equipment and more will all be controlled by simply making a gesture with an arm or using apps installed on the watch. Soon the smartwatch will be the only key anyone needs, the technology passport that gives access and control of your entire life.

Sensory data is also a rapidly growing market for wearable tech. Sensors built into a smartwatch or clothing will collect and process environmental factors such as humidity, pressure and temperature in addition to health data points. Everyone's local weather info can then be collated together and stored in the cloud to produce a micro-climate model. This would enable closer, more accurate measurement of air pollution and even plants could be watered automatically depending on conditions.

THE NXP DIFFERENCE

NXP powers and enriches the IoT as:

- The inventor of MIFARE, the world's leading technology for smartcard authentication
- The co-inventor of Near Field Communication (NFC), the wireless proximity technology bringing new levels of simplicity and security to interactions of all kinds
- A high-level contributor to standards bodies, including the FIDO Alliance, whose work promises to usher in a new era of online security, making the need to remember complex passwords a thing of the past.

The NXP Difference

NXP will help make these ideas into tomorrow's exciting reality as a supplier of end-to-end solutions that range from semiconductor ICs to infrastructure components and secure applications. We're the inventor of MIFARE, the world's leading technology for smartcard authentication, and the co-inventor of NFC, the wireless proximity technology bringing new levels of simplicity and security to interactions of all kinds.

As a proud employer of nearly 7,000 staff members in the United States, NXP is committed to security, leading-edge design, and bringing products to the domestic market that have a substantial share of domestically-built content and local value added to the end products in which NXP plays a role. Our company is dedicated to leveraging all of these resources and partnering with America's leaders to invest in this country's future and safer, more convenient lives for its citizens.

How to Reach Us:

NXP Semiconductors USA, Inc.
1455 Pennsylvania Avenue, NW, Suite 400,
Washington, DC 20004
Tel: +1.202.621.1831