Keywords: MAX66242, MAXQ610, home display unit, NFC/RFID authenticator IC, advanced metering infrastructure , DeepCover, Prepay utility service , Energy Prepay System,

APPLICATION NOTE 6163

LOOKING FOR AN ELECTRICAL PREPAYMENT SYSTEM IN YOUR HOME? NEAR-FIELD COMMUNICATIONS AND A SECURE AUTHENTICATOR

By: Hamed Sanogo, Executive Business Manager for Embedded Security Products, Maxim Integrated

Abstract: The adoption of the prepaid business model is actually growing with utility companies worldwide. The underlying technology of any prepaid utility program is smart meter technology, also known as advanced metering infrastructure (AMI), which enables real-time connectivity between customers and the utility company.

Background of an Energy Prepay System

Traditionally in the U.S., utility companies offering electric, water, and natural gas service have billed consumers on a postpaid basis. They track a customer's usage during the previous monthly or quarterly period, then send a bill based on that consumption. The customer is required to make payment within a predetermined time frame or risk having the electrical service disconnected.

We are all energy consumers, and some of us do not think about utility consumption (i.e., gas, heat, water) until the next bill arrives. But change is catching up. We are becoming more conscious of our consumption of natural resources and starting to be more thrifty and conservative. Many customers also want to take more control of the financial management of their utility bills. Enter a prepay system.

Prepay utility service has been popular for decades, particularly in Great Britain, Australia, New Zealand, Belgium, and South Africa. Meanwhile, the U.S. customer has generally only seen prepay service plans for cell phones, telephone cards, and bridge and highway tolls. The prepay utility option has also been a good model for those in remote areas, where investors do not always have a clear return on investment (ROI) for their investment outlays, and with transient populations like college students.

Customers can harness the power of an AMI system augmented with an HDU in their homes. To make the prepayment and reactivate the utility service, the system uses a secure NFC tag authenticator to ensure the security of the transaction.

Benefits of the Energy Prepay System

The consumer begins with a positive account balance; the utility company tracks real-time electrical usage and deducts the corresponding consumption charge from the prepaid credits. Fail to pay or to add more credits to an account, and service is terminated.

The adoption of the prepaid business model is actually growing with utility companies worldwide. Countless emerging economies are relying on this model as a way to invite many forms of investments in their countries. In particular, prepay electricity has become a worldwide growth trend. According to a report from Navigant Consulting (formerly Pike Research), the global installed base of prepaid metering customers is expected to grow from 31.7 million in 2014 to 85.2 million in 2024, with a compound annual growth rate (CAGR) of 10.4%. The same report predicts that for North America, the installed base of prepay meters is expected to grow from 650,000 to 3.1 million during the forecast period, with a CAGR of 17.0%.[1] As shown in **Figure 1**, the region with the most prepay customers forecasted is Asia Pacific.

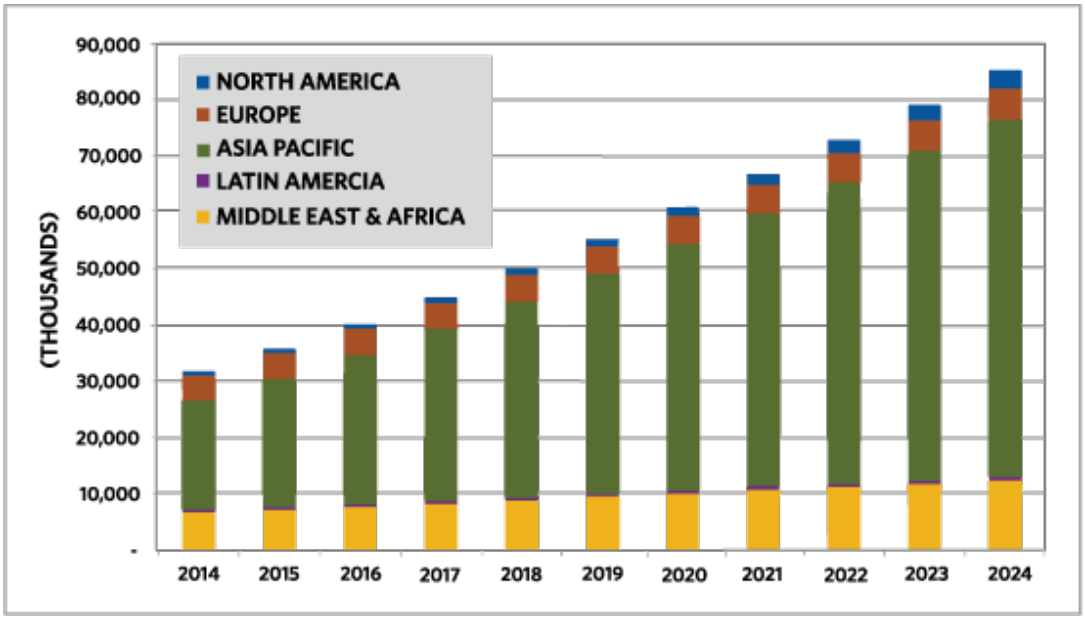

Figure 1. This chart from Navigant Research shows, "Prepaid Electric Meter Installed Base by Region, World Markets: 2014-2024."[1] Graphic supplied by Navigant Consulting Inc.

The prepay scheme allows utilities to easily reduce collection expenses; to reduce write-offs without the need to collect large deposits or disconnection fees; and to reduce bad debt by avoiding all the back-office and field activities associated with delinquent customers. They achieve a 100% collection rate immediately. Prepayment revenue arrives in advance of consumption, allowing utilities to invest and realize a predictable ROI. This model also eliminates the need to dispatch an employee to physically disconnect or reconnect service to a customer. With prepayment, there is no monthly billing statement to prepare. As a result, the utility reduces costly paperwork and the associated costs of postage, paper, printing, and handling.

Why do customers want to prepay? The short answer is that it provides the best means for easy monitoring of utility consumption. No more deposits, credit checks, due dates, or late fees! No more cancellation or

reconnection fees, no billing surprises, and 24/7 payment options over the Internet with smartphones. The prepay model empowers customers who want to consume electricity wisely with the means to do so. It gives customers the opportunity to manage their bills and electricity usage with a greater awareness of their usage patterns. It helps to foster a better understanding of the greater good of energy/fuel conservation.

We have witnessed human behavior change with new technology trends many times in the past. It is fair to assume that when customers can see their daily energy usage and costs on a home energy-monitoring device, they can be inspired to change their consumption patterns and habits.

The Infrastructure for an Energy Prepay System

Advanced Metering Infrastructure (AMI)

The underlying technology of any prepaid utility program is smart meter technology, also known as advanced metering infrastructure (AMI), which enables real-time connectivity between customers and the utility company. At its core is a digital meter (commonly called a smart meter) with remote disconnect and reconnect capabilities.

This two-way communication network between the utility's back office and the deployed smart meter is how consumption data and remote disconnect/reconnect commands are transmitted in real time. Using an AMI, utilities can now collect meter readings from the smart meters at predefined intervals that can be as short as a few minutes or even less. This is also how the utility can charge tariffs or implement upgrades to the meter's software.

Another essential companion component of the AMI is a separate pluggable energy-monitoring home display unit (HDU) located inside the customer's home.

Home Display Unit (HUD)

The customer's HDU (**Figure 2**) is essentially a power-status monitoring device, the two-way communications portal between the customer and the utility. The HDU is NFC enabled. A customer can use their smartphone or tablet platform to buy additional energy credits through an established Wi-Fi® or cellular network, then transfer these credits from the smartphone onto the HDU by using the NFC interface in the smartphone.

Figure 2. Demo board for a NFC-based prepay home display unit (HDU). The HDU communicates with the utility's back office to update the remaining energy credits. The transaction uses powerline communication (PLC) across the home's existing electric wiring.

This HDU demo platform was built to illustrate how the system works. Central to the HDU is the MAX66242 secure NFC tag authenticator. All the pieces of the demonstration unit are shown in **Figure 3**. The LCD displays the kilowatts consumed and the amount of kilowatt credits remaining. A switch enables or disables energy consumption. Operating this HDU requires a smartphone with NFC capability. A local Wi-Fi network connected to a laptop simulates the utility company's server. A travel router, MWR102 from ZyXEL, was used. The server runs a TCP/IP client-server app which handles the energy credit transactions. The server also has the meter's ROM ID, binding page data, partial secret, master secret (M-Secret), and page data (i.e., meter reading) so it can recreate each slave's secret (S-Secret). In this system, the HDU is the slave device while the server is the master.

Figure 3. The prepay utility demonstration platform presented here features the MAX66242 secure authenticator tag and a MAXQ610 microcontroller (not seen here).

The HDU displays customer energy consumption and expenditure information. Using the software app supplied by the utility, a customer can access their daily, hourly, or instant electricity consumption; thus, giving them the opportunity to analyze and perhaps change their energy-consumption behavior and even reduce their budget. Communication between the smart meter and the HDU can also be a hardwired connection through the existing electrical wiring from a power outlet using powerline carriers (i.e., powerline communication, PLC).

The utility can use the HDU to send the customer an audible alert when their account reaches a predetermined, low-balance amount. Customers can also choose to receive this notice by email, text message, phone call, or all three. A customer purchases additional credits at any time using the NFC-enabled smartphone/tablet. Replenished prepayment credits are then loaded onto the HDU. If a customer's prepaid balance is ever totally depleted, the HDU's display could be designed to turn red and service is disconnected shortly thereafter. After another prepayment, the account is remotely reconnected.

The HDU Architecture and Principles of Operation

Figure 4 shows the actual demonstration HDU, front side and back, built on the MAX66242 evaluation (EV) kit board. This architecture uses a DeepCover® secure, ISO/IEC 15693 tag authenticator IC, the MAX66242, to implement the energy prepayment system. The display panel was added to the EV kit board to facilitate the two-way communication.

Security is paramount in this energy prepay system. This HDU uses both the integrated SHA-256 crypto block technology in the MAX66242 secure tag and its memory protection features to ensure that the depletion and recharge of the energy prepayments do not expose the entire communication to counterfeiters and/or anyone who would exploit the exchange of private information.

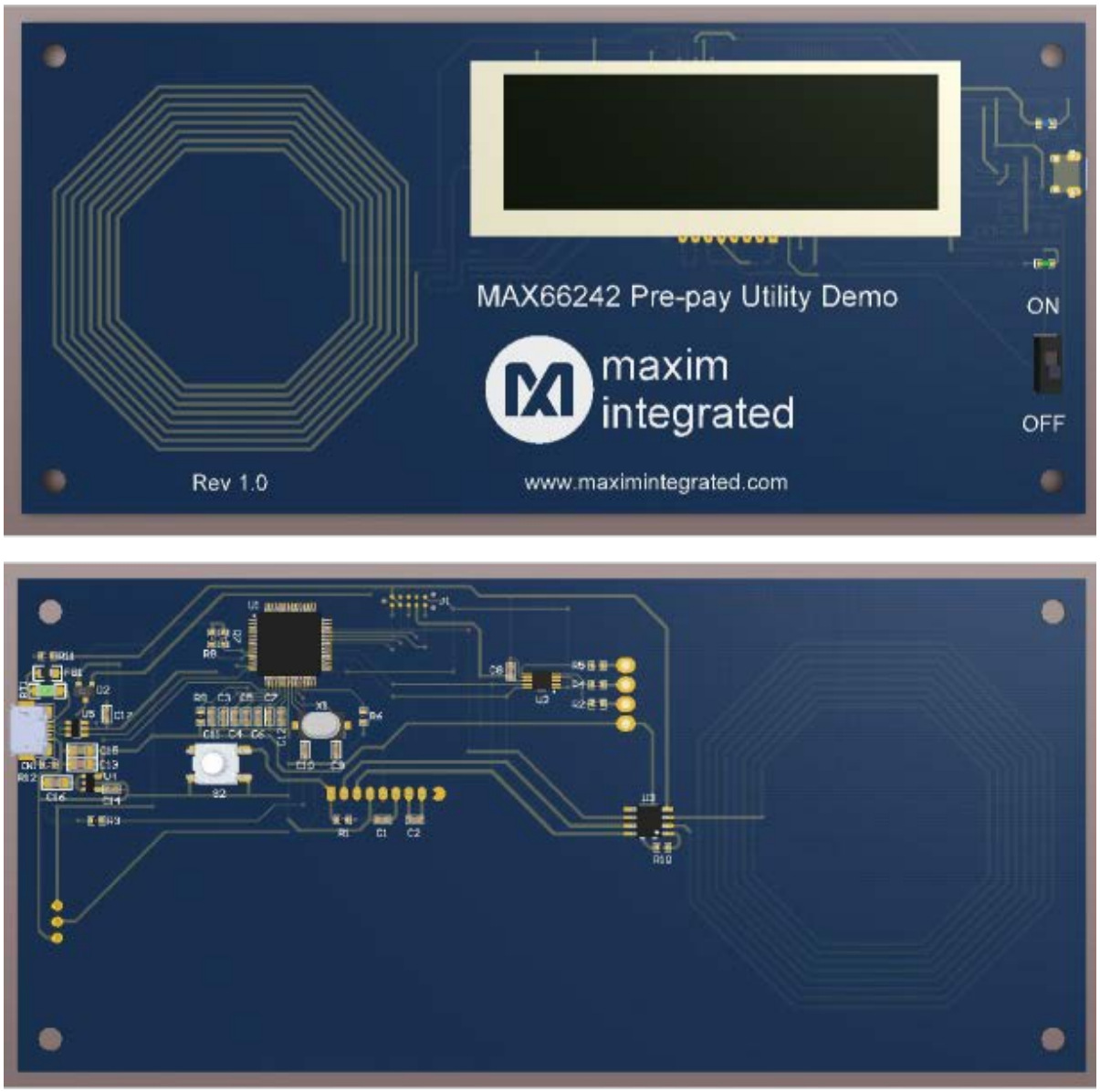

Figure 4. HDU front-side PCB (top) with integrated NFC antenna and display; HDU back-side PCB (bottom) shows the NFC antenna coil connected to the MAX66242 secure tag authenticator.

Actual system operation is surprisingly uncomplicated. First, the customer prepays for energy credits with a smartphone using a utility-supplied software app (**Figure 5** in Steps 1 and 2). Second, the customer aligns the smartphone's NFC antenna with the octagonal shaped antenna of the HDU. A handshaking transaction occurs between the phone and HDU, transferring the purchased credits from the smartphone securely onto the HDU (Step #3). Third, now the customer's account is updated with the amount of electricity prepaid credits, and the total available credit is updated instantly on the HDU's display screen. The remote connect and disconnect switch is then activated in Step 4 for a customer who is adding energy credits to an already

disconnected home. While updates from the smart meter to the HDU are done through the link in Step 5, the meter data is synchronized to the utility's server as seen in Step 6. Note that the current demo platform implementation does not allow the same smartphone to buy new energy credits unless the previously purchased credits have been transferred onto an HDU device.

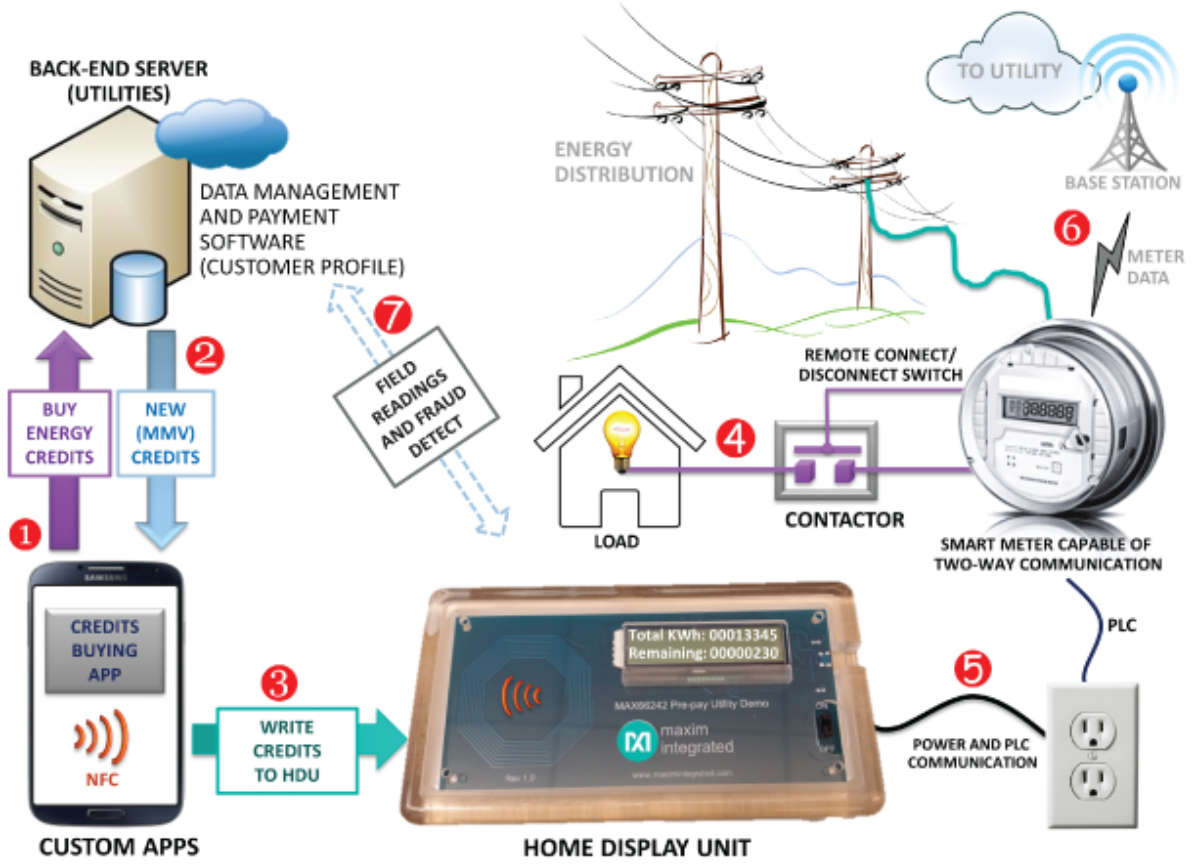

Figure 5. Advanced prepaid metering infrastructure showing energy buying framework. In Step 1, the customer uses the custom app and buys credits with a financial data transfer to the utility back-office servers. The prepayment credits (data packet including the maximum meter value, or MMV) are transferred to the smartphone in Step 2. The customer then transfers these credits onto their HDU in Step 3.

Operates over a Standard Wireless Network

This energy prepay system can be set up quickly without a full AMI deployment by using the ubiquitous wireless network around us (**Figure 6**).

The customer would first need to register for the prepaid system with the utility by completing a short profile. The credentials entered into the short profile are then used to set up the account and activate the payment system framework. The utility stores a secret in an HDU (i.e., the S-Secret), then sends the HDU to the customer. If the customer requests it, the utility can dispatch a technician to the customer's home to complete the hardware install.

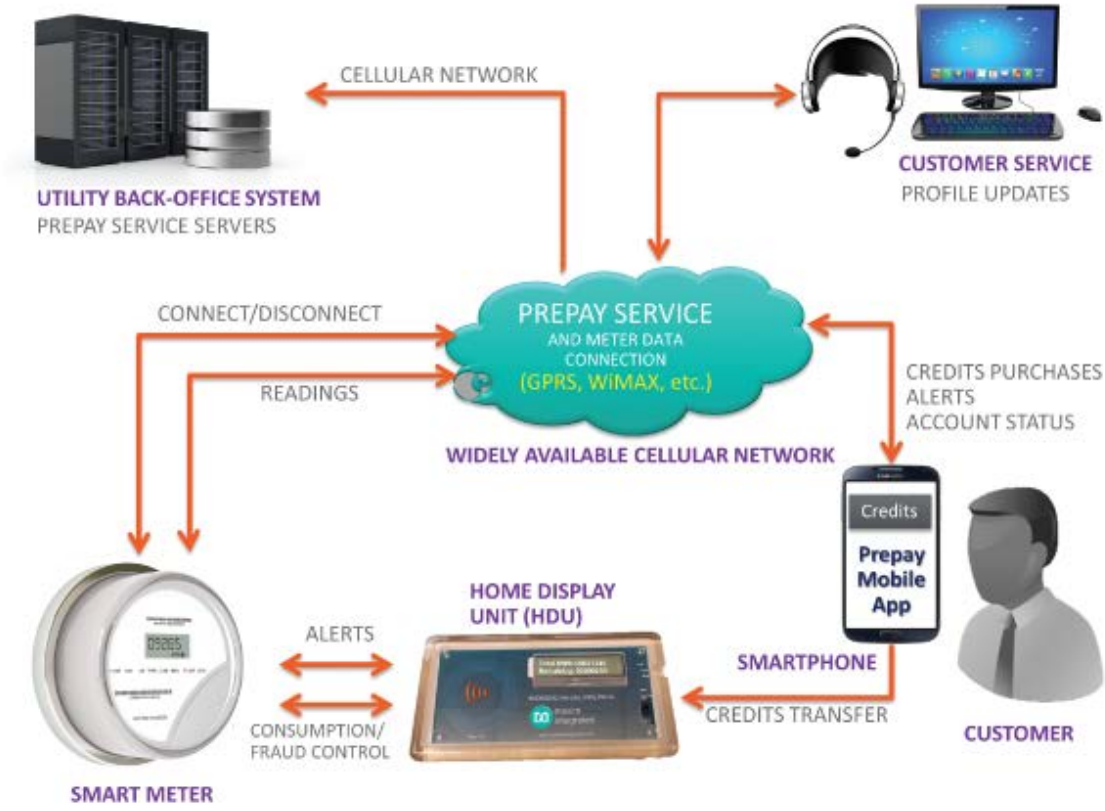

Figure 6. Prepayment system framework uses standard wireless PLC to communicate between the HDU and utility office.

Figure 6 shows how meter readings are communicated back to a collection point or cloud over the public wireless data or cellular network. Alerts, consumption data, disconnect/reconnect, meter fraud-checking commands are all transferred between the smart meter and the HDU. Just like the HDU, the prepaid phone app allows customers to access their prepaid balance, usage history, and other account information in real time. The information which flows from the utility back office to the HDU includes alerts to notify customers of low balance, disconnect, and other account information.

This approach offers utilities a seamless, scalable method for implementing a prepaid service program with a widely available wireless network. Eventually, this setup can be migrated to a full AMI deployment.

Securing the Energy Prepay Transaction

Securing these financial transactions requires the MAX66242, which is the key electronic component inside the HDU. This tag authenticator IC combines a wireless NFC/RFID interface with an I^2C interface. A 32-byte SRAM buffer facilitates fast data transactions over the I^2C interface. The IC has a crypto engine and user memory with protection modes that make it the best and most secure solution for hiding information on the HDU. The MAX66242 also has built-in hardware protection features, including proprietary die-level physical techniques, circuits, and crypto methods that isolate the HDU and protect it from tampering or being compromised by hackers or malicious attackers.

The MAX66242 essentially plays the role of a *secure element* inside the HDU. The integrated SHA-256 crypto engine provides symmetric challenge-and-response authentication (Figure 7) based on a secret key shared between the utility company's back-office servers (as master) and the HDU (as slave). While the secure server at the utility's back office implements the M-Secret function of this system, the S-Secret resides on the HDU at the customer's home inside the MAX66242. The same secret is computed by the utility's servers from the M-Secret that they maintained. The HDU has the S-Secret key in this authentication protocol. It is assumed here that the server derives the HDU's secret using data from the customer's profile. This SHA-256 hash algorithm is based on a secure hashing standard, publication FIPS PUB 180-4, defined by the National Institute of Standards and Technology (NIST), and it makes for a strong anti-counterfeiting or anti-cloning tool.

The HDU platform is illustrated in **Figure 7**. There are four data bytes in the HDU's (MAX66242) user memory which store the maximum kilowatt hour (kWh) value of the energy meter. We refer to this as the maximum meter value (MMV). Unlike a scheme where credit is loaded and then depleted as energy is consumed, the scheme used in this case is additive. When the customer buys (prepays) new credits, the total overall credit amount increases by the new amount. So, this MMV is the highest kilowatt hour reading allowed by the prepaid credits and, when reached, power is disconnected. The scheme used here computes its SHA-256 operation using a memory page in the MAX66242, which has been set to the *authentication protected* mode. (This is one of many memory protection modes supported by the IC.) The scheme also allows each HDU to have its own unique S-Secret based on the M-Secret placed on the server. Again, the smartphone is only a path, a conduit of information, in this scheme.

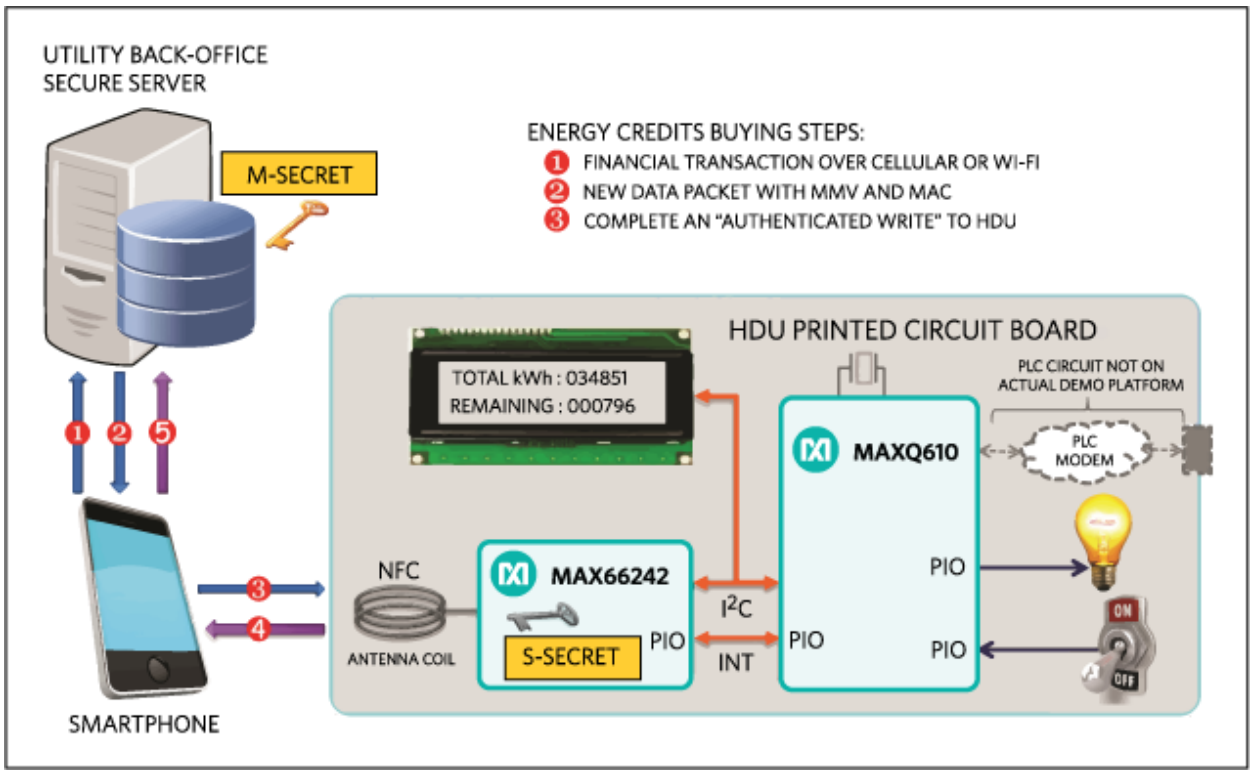

Figure 7. Block diagram of the HDU. The server computes the slave secret (S-Secret) from the master secret (M-Secret) using the customer-specific profile data that contains the HUD's ROM ID.

Since a customer profile was created when the customer first signed up with the utility company, the customer is known by the system. The back-office server now has the customer's personal information (e.g., name, address, etc.), MMV (initially zero for new customers), the HDU's ROM ID, and the selected memory-page data information from their profile. To purchase energy credits, the customer follows the transaction flow shown in Figure 7.

1. The customer uses an NFC-enabled smartphone or tablet loaded with a custom app to prepay energy credits (e.g., 1000kWh). In this case the app buys these credits directly from the utility through the customers' cellular data plan or home Wi-Fi connection. The utility's app guides the customer to do this. Once the server has implemented the transaction and verified that the payment has processed successfully, the server increments the MMV by the amount of energy credits prepaid by the customer.
2. The server then generates a data packet consisting of the new page data (i.e., a new MMV) and a corresponding computed message authentication code (MAC) to be used for an *authenticated write* action to the HDU's MAX66242. The server transmits the packet through the established cellular data or Wi-Fi connection to the smartphone.
3. The customer is now ready to transfer the purchased credits from the smartphone onto the HDU using the NFC interface. As explained in the nonfiction fable at the outset, the customer simply brings the smartphone near the HDU's antenna. The best and most reliable connection is when the smartphone's NFC antenna and the HDU's octagonal antenna are optimally aligned. The smartphone then writes the new MMV (e.g., 1000kWh) to the HDU (specifically, to the MAX66242 memory page) using an authenticated write along with the message authentication code (MAC) provided by the server. (Please note that the NFC smartphone is just a conduit for doing this authentication; it does not have the M-Secret nor does it have any knowledge of it.) Once this memory authentication is complete, the smartphone sends a short high-frequency (HF) message alerting the HDU that the transfer is complete. This short HF message toggles the PIO pin on the MAX66242, and the HDU's microcontroller (the MAXQ610) interprets this interrupt as an indication that a new set of energy credits is available. The microcontroller then reads the MAX66242 memory page and updates its own copy of the MMV. Only the server with the M-Secret can make this update, which is now displayed on the HDU's screen for the customer. The kilowatts remaining are recalculated and displayed.

Field Readings: Controlling Fraud and Electricity Theft

Occasionally, to ensure that a security breach has not happened to the smart meters and/or HDU, the utility company needs to perform field readings. (Refer to step 7 in Figure 5.) Field readings identify mismatches between the MMV value stored on the utility company's server and the one stored in the HDU. The HDU's MMV readings should never exceed the MMV stored on the server, so any mismatch between these two numbers indicates a tamper or even theft of electricity.

The field readings collect the total kilowatt hours currently stored in the HDU and upload it to the utility's server. There are two ways to collect field data: use PLC communication to link the smart energy meter to the HDU through the house's electrical lines, or let a service technician come and use a smartphone. The steps shown in **Figure 8** represent the field reading transaction implemented on the HDU demonstration platform.

1. The field technician uses a smartphone app to authenticate the meter by requesting a random challenge from the utility's server.
2. The smartphone instructs the HDU to perform a "Compute and Read Page MAC" for the memory page containing the MMV.

3. The smartphone sends the resulting MAC to the utility's server to validate the meter's authenticity. This method keeps the smartphone from knowing the M-Secret.
4. The utility's server computes its own MAC and compares it with the MAC received from the HDU.
5. If the two MACs match, the server responds with a "Good HDU" message to the smartphone. This means that the HDU is in good working order and has not been tampered with. If, however, the authentication process is not successful, this means that the HDU has been tampered with.

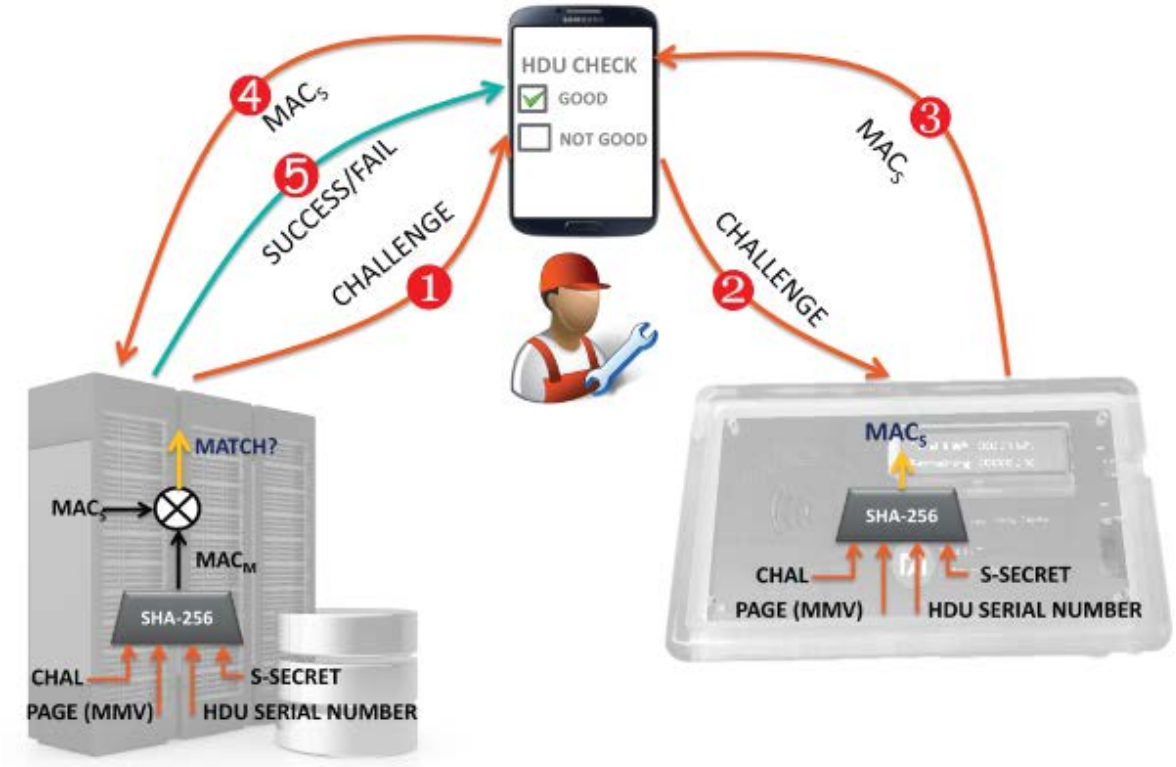

Figure 8. Service technician's checks for fraud. Any HDUs identified with this process would be removed from the field.

Conclusion

An electrical prepay system allows customers to choose when they pay, how they pay, and drives how much they consume allowing customers to take more control of their bills and utility usage because customers become more cognizant of their energy use over time.

In areas like the U.K., Australia, and New Zealand where a prepay energy credit system exists today, customers know how much it costs to run certain appliances and they can relate that to a specific amount per day for electricity. This leads to the adoption of conservation measures, including turning off appliances, turning down a water heater, purchasing Green Star appliances, installing energy-efficient bulbs.

Advanced smart metering infrastructure (AMI) systems outfitted with two-way communications, a remote disconnect switch, and an HDU with the DeepCover secure MAX66242 NFC tag authenticator provides an effective energy prepayment system. Such a framework helps utilities simplify business operational efforts,

cut costs, reduce delinquent account risks, improve cash flow, provide immediate customer service, and encourage conservation. Simply put, this is a prepayment system which creates a win-win-win situation for the utilities, the consumers, and the world's resources.

Reference

1. "Prepaid Electric Metering," **Pike Research**, March 2012, http://www.navigantresearch.com/wp-content/uploads/2012/03/PPM-12-Executive-Summary2.pdf

An article similar to this application note was published in EDN.com, July 2015.

Related Parts		
MAX66242	DeepCover Secure Authenticator with ISO 15693, I²C, SHA-256, and 4Kb User EEPROM	Free Samples
MAXQ610	16-Bit Microcontroller with Infrared Module	Free Samples

More Information
For Technical Support: https://www.maximintegrated.com/en/support
For Samples: https://www.maximintegrated.com/en/samples
Other Questions and Comments: https://www.maximintegrated.com/en/contact

Application Note 6163: https://www.maximintegrated.com/en/an6163
APPLICATION NOTE 6163, AN6163, AN 6163, APP6163, Appnote6163, Appnote 6163