INTRODUCTION
The RFID tags we consider are small, cheap, and passive radio-readable labels. The tags are powered through induction from a reader field, whose strength decreases rapidly with the distance between tag and reader. Hence, a tag’s maximal reading distance depends on its received power consumption and roughly halves when the tag requires more received power. Each tag has a unique identification number, which can be read by the reader. The reader uses this ID to obtain information from a backend database. The most severely constrained tags are those used in logistics applications such as Electronic Product Code (EPC) tags. Logistics tags must use very little power in order to achieve sufficient reading ranges and must be very cheap to be affordable for tagging of low-cost items. Advances in chip scaling would make tags with increasingly more transistors affordable for low-cost applications, but, as of yet, not enough power is available on the tag to supply the additional circuitry. Any privacy and security measure on RFID tags, therefore, has to be low power and low area to achieve acceptable reading ranges.

The basic tags in circulation today provide no privacy and security protection; any reader can read the unique ID from the tag and look up information in often public databases. One system that causes such direct information disclosure is the planned Object Name Service (ONS) system designed by EPC global, which uses the Internet Domain Name System (DNS) to locate product information about tagged items [1]. To locate the right ONS server, the system requires that the tag IDs be highly structured (e.g., the same products need to have the same ID prefix), thus leaking significant information even when only small parts of an ID are disclosed. The first steps towards more privacy are to restrict access to the back-end databases and to use unstructured ID numbers.

Even with random IDs and no publicly available metadata, information can be deduced from the tags. In particular, if a tag with a static identifier is read at different times or in different locations, an adversary can trace its movement through the physical world. These traces of RFID movement are similar to Internet traces that record the web pages a user has visited [2]. In the same way that Internet traces have a value and are actively traded [3], we hypothesize that RFID traces also have a value that makes them worth collecting. Applications in which RFID traces can be used include surveillance of individuals and corporate spying. Competitors can, for example, estimate a merchant’s turnover by repeatedly browsing through
the aisles and reading the tags. Just as Internet traces are increasingly used to derive information about a user’s preferences, the movement of individuals can encode information about their shopping behavior, price sensitivity, taste, and many other items of personal information. The information can be used to implement profit-maximizing schemes, including price discrimination and targeted advertising. It should, thus, be desirable for corporations and individuals to control and restrict access to their RFID tags.

**RFID Privacy and Security**

RFID tags constitute a privacy and security risk if individuals can be tracked or internal business processes can be monitored through the tags. Hence, privacy and security requires that different RFID tags cannot be distinguished by rogue readers. Privacy and security can be achieved through public key cryptography. Users would concatenate their ID with a random number and encrypt it with the public key of the database. Only the legitimate database could decrypt the response to determine the ID. Public key encryption, however, cannot be implemented on small devices. Hardware implementations of public key ciphers are at least six orders of magnitude more expensive than symmetric primitives such as block ciphers, stream ciphers, and hash functions. Even optimized silicon implementations currently exceed the power budget by several orders of magnitude. These optimized implementations will likely not become sufficiently power efficient for many years, because of a fixed power overhead caused by the analog front-end and other parts of the chip, and because of diminishing scaling effects [4]. While the active power consumption of each transistor decreases with its size, leakage increases exponentially in smaller technologies thereby offsetting the gain in power efficiency. In order to fit in the power budget of today’s RFID chips, all the protocols we consider employ hash functions and use symmetric keys shared between the tag and legitimate readers. Research into RFID privacy over the past several years has produced a number of possible protection schemes. Early proposals such as breaking or deactivating those tags that leave the domain of the owner—typically at check-out time [5]—have meanwhile been integrated into some RFID standards including EPC Gen2 [6].
These simple solutions sacrifice the possibility of post sales applications including smart homes and warranty management and are not widely used in practice. Other RFID applications such as payment tokens and passports require the tags to remain active when given to individuals and therefore need more elaborate privacy protection schemes. Furthermore, deactivating tags does not provide any protection from the corporate espionage that would happen before checkout.