

RFID TECHNICAL TUTORIAL

Dale R. Thompson
Department of Computer Science and Computer Engineering
University of Arkansas
Fayetteville, Arkansas 72701
(479) 575-5090
drt@uark.edu

Radio frequency identification (RFID) uses radio frequency signals to automatically identify objects. RFID is used to pay for gas without going into the store, in automobile immobilizer systems to prevent theft, in toll road systems to automatically pay tolls without stopping, in animal identification, in secure entry cards, and in the supply chain to manage the flow of pallets, cases, and items. Most media accounts of RFID are actually about one form of RFID the electronic product code (EPC) system used by retailers to manage the supply chain. EPC has standardized chip designs and protocols that have enabled the mass production of low-cost passive RFID tags. EPC provides identification of the product to which the EPC tag is attached like a barcode, except that it can be read at a distance and does not require line-of-sight aiming.

This technical tutorial describes how RFID systems work with emphasis on the EPC system used by retailers. It begins by describing several applications of RFID. Then, the tags, readers, and data link protocols are described. Existing and emerging standards from the ISO and EPCglobal are discussed. EPCglobal Inc. is a global not-for-profit standards organization commercializing the Electronic Product Code™ (EPC) and RFID worldwide. The EPC system is emphasized because the mass production of EPC tags is creating the largest RFID system that will have a long-term impact on society. The three UHF passive tag standards supported by EPCglobal named Class-0, Class-1 Generation 1 (Gen-1), and Class-1 Gen-2 are presented.

The tutorial concludes by discussing security and privacy issues. The retail industry is concerned if an attacker either performs an unauthorized inventory or disrupts business operations by modifying or deleting the serial number of an RFID tag. However, the privacy of an individual is of concern when objects can be identified with a no-contact and non-line-of-sight RFID system. Privacy advocates are concerned if an attacker either plants a smart bomb that explodes when there are five or more Americans with RFID-enabled passports detected in a restaurant or if a sufficiently powerful directed reader reads tags in a house or car. Threats to an RFID system and threats by an RFID system to privacy are discussed. Threats are potential events that cause a system to respond in an unexpected or damaging way. Different threats are categorized as the first step in threat modeling, which is a formal security-based analysis to determine the highest level security risks to a system. A secure RFID system that protects the privacy of individuals cannot be built unless the threats are understood.