

1.0 Problem Statement

[Return to User Scenario: Identity](#)

Nancy is a USA citizen and plans a month-long European vacation with 4 major legs all within the Schengen Agreement Zone¹⁾.

Many companies have adopted [Multifactor Authentication \(MFA\)](#) to help avoid fraudulent activities. MFA relies on three main factors in determining the authenticity of a user²⁾:

- **Knowledge Factors** include all things users must know in order to log in to gain access to a system. This includes Usernames, IDs (i.e., Passport or Driver's license numbers), passwords, and personal identification numbers (PINs), answers to security questions(i.e., your favorite sport), or information derived from PII (i.e., mother's maiden name, oldest child's middle name).
- **Possession Factors** consist of things users must have in their possession in order to log in. This includes one-time password tokens, key fobs, smartphone apps, and employee ID cards. These all work well until those things go missing as a result of negligence, lost baggage, direct or indirect theft. Direct theft is when the Possession Factor is taken directly (i.e., the intent of the theft), indirect is when the Possession Factor is taken collaterally (i.e., handbag theft)
- **Inherence Factors** include characteristics inherent to individuals confirming their identity. This includes the scope of biometrics, such as retina scans, fingerprint scans, facial recognition, and voice authentication.

MFA can use other attributes about any transaction:

- **Location Factors** include using the user's current geographic location as determined by Global Positioning System (GPS) or using mobile device radio tower triangulation. Location Factors are generally not used as a sole source of identification but are used in combination with other identifying factors such as Knowledge, Possession, or Inherence. For example, an attempt is made to sign-on to a site using the user's user id and password but is doing so from a different location. The server rejects the sign-on because it uses the combination of the user/password and location to confirm the identity of the user.

such as a physical location, computing device, network, or database. While Nancy is at home, in the USA using her own network and computer, the likelihood of any issues is small. However, as Nancy travels MFA can prohibit her from being able to access or update her information because of Locations Factors and Time Factors. This is why it is essential for Nancy to notify her Credit Card companies and banking institutions about her proposed itinerary.

Nancy needs to identify herself while planning for the trip and during the trip, potentially exposing a lot of [Personal Identifiable Information \(PII\)](#), [Digital Signature](#) as well as financial information (i.e., Credit Cards, Debit Cards, etc.) to numerous people in numerous countries from the beginning to the end. In addition to the exposure of her PII to the corporations, businesses, and individuals that she has direct business with, she also has to worry about her PII being processed by partner organizations working with businesses she is working with. As a result of poor [Data Residency](#) requirements, her PII might be processed and stored across the world thus limiting her ability for recourse if there are compromises. See [4.3.4.1 Confidentiality](#).

An overview of the trip is:

1. A river cruise along the Rhine River visiting some major cities, villages, and historic sites
2. A Paris getaway with cultural, shopping, eating, and clubbing activities
3. A mountain resort adventure with hiking, skydiving, paddleboarding, water skiing, and kayaking
4. A casino experience with shows, clubbing, and gambling
5. Nancy does all the bookings in advance for:
 1. Airplane
 2. Cruise ships
 3. Trains
 4. Hotel In Paris
 1. Museum visits
 2. Historical Sights
 3. Restaurants
 4. Discotheque
 5. Resort with some activities such as a
 1. Hiking
 2. Sky Diving
 3. Paddle Boarding
 4. Water Skiing
 5. Kayaking
 6. Casino
 1. Discotheque
 2. Cabaret shows
 7. Long Term Parking

1)

Schengen Agreement, allows passport-free travel between these 26 countries: Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden, and Switzerland. There are three islands that are also part of the Schengen Zone, even though their borders are outside of the continent: The Azores, Madeira, and the Canary Islands.

2)

Mary E. Shacklett, TechTarget, Multifaactor Authrtication, Accessed: 24 June 2021, <https://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA>

From:
<https://www.omgwiki.org/dido/> - **DIDO Wiki**

Permanent link:
https://www.omgwiki.org/dido/doku.php?id=dido:public:s_cli:05_contents:02_prt:identity:01_problem:start&rev=1624557800

Last update: 2021/06/24 14:03

