	Biometrics	Behavioral Biometrics	Contextual Multi-dimensional Authentication (CMA)
Market entry	**Early 2000**	**Around 2010**	**2018**
Authentication format	**Static** (Fingerprint, facial recognition, voice, Iris)	**Dynamic** (continuous touch, scroll, pressure, size,)	**Contextual** Includes Static+ Dynamic + Contextual
Multi-factor authentication	**1 Factor** (Something you are)	**1 Factor** (Something you are, something you have)	**3 Factor** Something you are, something you know and something you have
One-time authentication Vs. continuous authentication	**One-time authentication**	**Continuous authentication,**	**Continuous authentication,**
User involvement (confidence factor)	Yes	No	Contextual – Can be yes/no
Functional from day 1?	Yes (but can be hacked) – Same device	No (learning curve)	Yes
User perception	User feels protected as he needs to explicitly authenticate	User may feel unprotected he authenticates without knowledge	User feels protected as he in certain situations needs to generate step-up authentication
Security level	Low (when using same device) Have ability to fall back to password. **Not real security**	Medium-high	High
False positive	**Low**	**Medium (but take time to learn)**	**Low**
Identity and privacy	**Medium**	**Medium**	**High (hybrid)**
How decision is generated	Sensor interaction	Sensor interaction + Machine learning (based on device sensors)	Smart rules + advanced machine learning
Detection during the Users journey	**Login/transaction (2 stages)**	**Registration/ Transaction (2 stages)**	**All four stages**
Friction level	**High**	**Low**	**Low**