**Verschiedene Alternativen im Überblick**

**Karten mit ein- und auschecken**

Um in den Park zu kommen muss der Nutzer mit einer Karte in den Park einchecken. Nach dem Einchecken ist kein weiteres Eintreten in den Park möglich. Sobald der Nutzer diese Karte zum Auschecken aus dem Park nutzt, wird die Sperrung zum Einchecken entfernt, wodurch ein erneutes Eintreten möglich ist. Sollte der Nutzer einen anderen Ausgang wählen, wodurch kein Auschecken möglich ist, wird die Karte nach einer Zeit x oder zu einem Zeitpunkt x entsperrt, wodurch anschließend ein Einchecken in den Park wieder möglich ist.

|  |  |
| --- | --- |
| PRO | CONTRA |
| unkomplizierte Entwicklung | Karten gehen leicht verloren -> Mitarbeiter für Sperrung nötig |
| einfache Anwendung | Karten müssen produziert werden |
| nicht so datenschutzkritisch | Karte kann weitergegeben werden |

**Gesichtserkennung**

Um den Park zu betreten wird das Gesicht analysiert und bewertet, ob diese Person eine Jahreskarte besitzt. Nachdem der Nutzer in den Park eingetreten ist, wird diese Person für einen weiteren Eintritt innerhalb der Zeit x gesperrt.

|  |  |
| --- | --- |
| PRO | CONTRA |
| Biometrisch | Datenschutzkritisch |
| „Austricksen“ aufwändiger | noch nicht ausgereift |
| Bibliotheken zum Entwickeln existieren bereits | Eintrittsvorgang zeitaufwendig |

Anmerkung: Experiment am Südkreuz

**Fingerabdruck**

Um den Park zu betreten wird der Fingerabdruck analysiert und bewertet, ob diese Person eine Jahreskarte besitzt. Nachdem der Nutzer in den Park eingetreten ist, wird diese Person für einen weiteren Eintritt innerhalb der Zeit x gesperrt.

|  |  |
| --- | --- |
| PRO | CONTRA |
| Biometrisch | Datenschutzkritisch |
| „Austricksen“ aufwändiger |  |

**Personalausweis mit Nummer**

Um den Park zu betreten wird geprüft, ob der Nutzer mit dieser Personalausweisnummer eine Jahreskarte besitzt. Nachdem der Nutzer in den Park eingetreten ist, wird diese Person für einen weiteren Eintritt innerhalb der Zeit x gesperrt.

|  |  |
| --- | --- |
| PRO | CONTRA |
| Eindeutig | Personalausweis kann weitergegeben werden |
| nicht so Datenschutzkritisch |  |
| mit passendem Lesegerät, sollte Implementierung „leicht“ sein |  |
| für alle Arten von Personalausweis innerhalb Deutschlands nutzbar (alt & neu) |  |
| Personalausweis normalerweise am Mann |  |

**Personalausweis mit Fingerabdruck**

Um den Park zu betreten wird geprüft, ob der Nutzer denselben Fingerabdruck hat, wie dieser, der auf dem Personalausweis gespeichert ist. Zudem wird geprüft, ob dieser Nutzer eine Jahreskarte hat. Nachdem der Nutzer in den Park eingetreten ist, wird diese Person für einen weiteren Eintritt innerhalb der Zeit x gesperrt.

|  |  |
| --- | --- |
| PRO | CONTRA |
| Biometrisch | nur neuer Ausweis nutzbar |
| nicht so Datenschutzkritisch | nur für Personen nutzbar, die den Fingerabdruck auf dem Ausweis speichern lassen haben |

**Handvenenerkennung**

Um den Park zu betreten wird geprüft, ob der Nutzer denselben Handvenenabdruck hat, wie der hinterlegte. Zudem wird geprüft, ob dieser Nutzer eine Jahreskarte hat. Nachdem der Nutzer in den Park eingetreten ist, wird diese Person für einen weiteren Eintritt innerhalb der Zeit x gesperrt.

|  |  |
| --- | --- |
| PRO | CONTRA |
| Keine Karte nötig (bei Serverlösung) | Hygiene |
| eindeutig | Datenschutz |
| Biometrisch |  |

**App**

Damit ein Nutzer in den Park eintreten kann, muss sich dieser mittels des Fingerabdrucks oder ähnlichem verifizieren. Anschließend wird ein QR-Code generiert, mit dem Eingetreten werden kann. Anschließend wird der Code ungültig und kann nicht mehr genutzt werden.

|  |  |
| --- | --- |
| PRO | CONTRA |
| einfache Anwendung für Nutzer | QR-Code kann weitergeschickt werden |
| „leicht“ zu implementieren | Mehrere Fingerabdrücke können gespeichert sein |

**Zeitkarte**

Es gibt eine Karte mit einem Barcode (zum Beispiel Studentenausweis). Mit diesem Barcode kann Zeit gekauft werden, die man im Park verbringen darf. Das heißt, beim Ein- und Austritt muss diese Karte gescannt werden.

Wichtige Anmerkungen: Sollte nur für HWR-Angehörige sein, da es eine Kooperation zwischen der HWR und dem Tierpark ist. Um Wirtschaftlichkeit zu gewährleisten ist die Karte nur für die Nutzung von Montag bis Freitag und nicht an Feiertagen gedacht.

|  |  |
| --- | --- |
| PRO | CONTRA |
| einfache Anwendung für Nutzer | Karte kann weitergegeben werden (hat aber weniger Nutzen) |
| „leicht“ zu implementieren | Bevorzugung von HWR-Angehörigen vor sonstigen Personen |

***Biometrische Datenspeicherung – Diskussion***

Bei den Alternativen Gesichtserkennung und Fingerabdruck stellt sich die Frage, wo die Vergleichsdaten liegen.

**Biometrische Datenspeicherung auf einer Karte**

Die biometrischen Vergleichsdaten werden auf einer Karte gespeichert, welche dem Nutzer ausgehändigt wird. Beim Eintrittsvorgang des Nutzers muss dieser die Karte einlesen lassen und entsprechendes biometrisches Merkmal von ihm prüfen lassen. Nachdem der Nutzer in den Park eingetreten ist, wird diese Person für einen weiteren Eintritt innerhalb der Zeit x gesperrt.

|  |  |
| --- | --- |
| PRO | CONTRA |
| keine Kommunikation zwischen Client und Server notwendig | Karten werden verloren |
| Datenschutz leichter einhaltbar | beide Merkmale in einer Hand -> leichtere Manipulation möglich |
|  | aktuelle Karten nicht nutzbar |

**Biometrische Datenspeicherung in einer Datenbank**

Die biometrischen Vergleichsdaten werden in einer Datenbank gespeichert. Der Nutzer muss beim Eintrittsvorgang das entsprechende biometrische Merkmal von ihm „einlesen“ lassen, welches anschließend mit der Datenbank verglichen wird. Nachdem der Nutzer in den Park eingetreten ist, wird diese Person für einen weiteren Eintritt innerhalb der Zeit x gesperrt.

|  |  |
| --- | --- |
| PRO | CONTRA |
| keine Karte kann verloren werden | zwingend sichere Verbindung zwischen Client und Server notwendig |
| Manipulation fast komplett ausgeschlossen | sehr Datenschutzkritisch |
| aktuelle Karte kann genutzt werden | Hochsicherheitsserver notwendig |