إنترنت الأشياء (IoT) هي عبارة عن مجموعة من الكائنات الجامدة مع اتصال لاسلكي مدمج ، يتم مراقبته والتحكم فيه وربطه عبر الإنترنت ، ولكن كما هو الحال مع أي تقنية جديدة ، قد يكون إنترنت الأشياء مربكًا بالنسبة إلى المستهلك ، لا سيما وأن المناقشات تدور حول الأمن والخصوصية. وعلاوة على ذلك ، فإن إنترنت الأشياء لديها العديد من التطبيقات مثل التشغيل الآلي للمنزل ، والرعاية الصحية ، والشبكة الذكية ، والمدينة الذكية والسيارات الذكية. التطبيقات التي تعتمد على تقنية انترنت الاشياء تولد كمية هائلة من البيانات وهذا يؤدي إلى العديد من المخاوف الأمنية مثل كيفية تأمين هذه الأجهزة والبيانات والاتصالات من الوصول غير المصرح به. تعد المصادقة بمثابة لبنة أساسية لتوفير المصادقة المتبادلة بين المستخدم والأجهزة في بيئة انترنت الاشياء. ومع ذلك ، فإن إنترنت الأشياء يتألف من أجهزة مقيدة في قدرتها الحسابية ، وعرض نطاق الشبكة ، والذاكرة ، مثل جهاز الاستشعار. لذلك ، في هذه الرسالة ، اقترحنا بروتوكول تبادل مفاتيح خفيف الوزن يستخدم شهادة ضمنية تتمتع بميزات كبيرة على الشهادات التقليدية. تسمح الشهادة الضمنية لمخططنا المقترح باستخدام حجم صغير من الحزمة المرسلة أثناء تشغيل المخطط المقترح ، مما يؤدي إلى توفير النطاق الترددي والذاكرة والطاقة. وفي الوقت نفسه ، يعتمد مخططنا المقترح على نظام تشفير المنحنى الإهليلجي الذي يسمح باستخدام حجم مفتاح صغير ، مما يحفظ موارد الشبكة ويقلل من تعقيد الحساب. يوفر المخطط المقترح مصادقة مفتاح واضحة مع تأكيد مفتاح جلسة العمل التي يمكن أن تصمد ضد هجوم رفض الخدمة في تطبيقات إنترنت الأشياء ، ولديه آلية للتحقق من هوية الشريك من حساب مفتاحه العام الثابت. بالإضافة إلى ذلك ، فإننا نستخدم أداة Scyther كأسلوب رسمي للتحقق التلقائي للتحليل والتحقق من المطالبات الأمنية للمخطط المقترح ، وتظهر النتائج أن مخططنا المقترح آمن في نموذج eCK. نحن نقارن المخطط المقترح مع المخططات الأخرى الموجودة في دراستنا من حيث الأمن والأداء ، ويظهر أن المخطط المقترح يلبي خصائص الأمان المرغوبة في بيئة إنترنت الأشياء .